Elliptic Curves

Dr T. Fisher

Lent 2008

LaTeXed by Sebastian Pancratz

These notes are based on a course of lectures given by Dr T. Fisher in Part III of the Mathematical Tripos at the University of Cambridge in the academic year 2007–2008.

These notes have not been checked by Dr T. Fisher and should not be regarded as official notes for the course. In particular, the responsibility for any errors is mine — please email Sebastian Pancratz (`sfp25`) with any comments or corrections.

Contents

1 Fermat's Method of Descent 1

2 Some Remarks on Plane Cubics 5

3 Weierstrass Equations 9

4 The Group Law 13

5 Isogenies 17

6 The Invariant Differential 21

7 Formal Groups 25

8 Elliptic Curves over Local Fields 29

9 Elliptic Curves over Number Fields: The Torsion Subgroup 35

10 Kummer Theory 39

11 Elliptic Curves over Number Fields: The Mordell–Weil Theorem 41

12 Heights 43

13 Dual Isogenies 47

14 Galois Cohomology 49

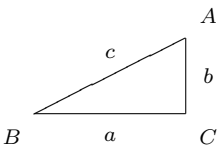
15 Weil Pairing 53

16 Decent by Cyclic Isogeny 57

Chapter 1

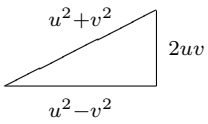
Fermat's Method of Descent

Consider a right-angled triangle ABC



with $a^2 + b^2 = c^2$ and area $(ABC) = ab/2$.

Lemma 1.1. Every primitive triangle is of the form



for some $u, v \in \mathbb{Z}$ with $u > v > 0$.

Proof. Without loss of generality, a is odd, b is even and c is odd. Now rewrite $a^2+b^2 = c^2$ as $\left(\frac{b}{2}\right)^2 = \frac{c+a}{2}\frac{c-a}{2}$ where $\frac{c\pm a}{2}$ are coprime positive integers with product a square. Unique factorisation in $\mathbb{Z}$ gives $\frac{c+a}{2} = u^2$, $\frac{c-a}{2} = v^2$ for some $u, v \in \mathbb{Z}$ so $a = u^2 - v^2$, $b = 2uv$, $c = u^2 + v^2$. □

Definition. $D \in \mathbb{Q}_{>0}$ is *congruent* if there is a rational triangle with area D.

Remark. It suffices to consider D a square-free integer.

Example. 5 and 6 are congruent numbers.

Remark. D is congruent if and only if $Dw^2 = uv(u^2 - v^2)$ for some $u, v, w \in \mathbb{Z}$ with $w \neq 0$, which is equivalent to $Dy^2 = x^3 - x$ by setting $x = u/v$, $y = w/v^2$ for some $x, y \in \mathbb{Q}$ with $y \neq 0$.

Theorem 1.2 (Fermat)**.** 1 is not congruent, that is, there is no solution to

$$w^2 = uv(u + v)(u - v) \qquad (*)$$

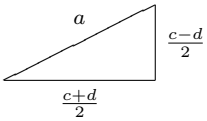
with $u, v, w \in \mathbb{Z}$ and $w \neq 0$.

Proof. Without loss of generality, u and v are coprime with $u > 0$. Moreover, if $v < 0$ then we replace (u, v) with $(-v, u)$, and if $u \equiv v \pmod 2$ then we replace (u, v, w) by $\left(\frac{u+v}{2}, \frac{u-v}{2}, \frac{w}{2}\right)$.

Now u, v, $u+v$ and $u-v$ are positive coprime integers with product a square. Unique factorisation in $\mathbb{Z}$ gives

$$u = a^2, \qquad v = b^2, \qquad u + v = c^2, \qquad u - v = d^2$$

for some $a, b, c, d \in \mathbb{N}$. As $u \not\equiv v \pmod 2$, c and d are odd. Consider the triangle



This is a primitive triangle with area

$$\frac{1}{2}\left(\frac{c+d}{2}\right)\left(\frac{c-d}{2}\right) = \frac{c^2-d^2}{8} = \frac{v}{4} = \left(\frac{b}{2}\right)^2.$$

Put $w_1 = b/2$ and note that this is an integer. By Lemma 1.1,

$$w_1^2 = u_1 v_1 (u_1^2 - v_1^2)$$

for some $u_1, v_1 \in \mathbb{Z}$. So (u_1, v_1, w_1) is another solution to $(*)$. But $4w_1^2 = b^2 = v \mid w^2$ so $|w_1| < |w|$. Thus, by Fermat's method if infinite descent, there are no solutions to $(*)$. □

Remark. For a right-angled triangle with sides a, b and c the three numbers $\left(\frac{a-b}{2}\right)^2$, $\left(\frac{c}{2}\right)^2$ and $\left(\frac{a+b}{2}\right)^2$ form an arithmetic progression of length 3 with common difference $D = ab/2$.

1.1 A Variant for Polynomials

Let K be a field with $\mathrm{char}(K) \neq 2$.

Theorem 1.3. Let $u, v \in K[t]$ be coprime. If $\alpha u + \beta v$ is a square for distinct ratios $(\alpha : \beta) \in \mathbb{P}^1$ then $u, v \in K$.

Proof. We may assume that $K = \bar{K}$. Changing coordinates on $\mathbb{P}^1$ via Möbius maps, we may assume that the four ratios are $(1:0)$, $(0:1$, $(1:-1)$ and $(1:-\lambda)$ for some $\lambda \in K$ with $\lambda \neq 0, 1$.

$$\begin{aligned} u &= a^2, & u - v &= c^2 = (a-b)(a+b) \\ v &= b^2, & u - \lambda v &= d^2 = (a-\mu b)(a+\mu b) \end{aligned}$$

where $\mu = \sqrt{\lambda}$. u and v are coprime so a and b are coprime, hence $a-b$ and $a+b$ are coprime. Unique factorisation in $K[t]$ gives that $a-b$ and $a+b$ are squares. Similarly, $a-\mu b$ and $a+\mu b$ are squares.

Now $\max\{\deg(a), \deg(b)\} < \max\{\deg(u), \deg(v)\}$ and so we are done by Fermat's method of infinite descent. □

Definition. (i) E/K is the projective closure of an affine curve $y^2 = f(x)$ where $f(X) \in K[X]$ is a monic degree 3 polynomial with distinct roots over $\bar{K}$.

(ii) For any field extension L/K,

$$E(L) = \{(x, y) \in L^2 : y^2 = f(x)\} \cup \{\mathcal{O}_E\}$$

where $\mathcal{O}_E$ is the point at infinity.

Fact. $E(L)$ is naturally an abelian group with identity $\mathcal{O}_E$.

Example. $E\colon y^2 = x^3 - x$, $E(\mathbb{Q}) = \{\mathcal{O}_E, (0,0), (\pm 1, 0)\}$.

Corollary 1.4. If E/K is an elliptic curve then $E(K(t)) = E(K)$.

Proof. Without loss of generality, $K = \bar{K}$. By substitutions in x, we may assume E is of the form $E\colon y^2 = x(x-1)(x-\lambda)$ for some $\lambda \in K - \{0, 1\}$. If $(x, y) \in E(K(t))$, write $x = u/v$ with $u, v \in K[t]$ coprime so that $w^2 = uv(u - v)(u - \lambda v)$ for some $w \in K[t]$. Unique factorisation in $K[t]$ implies that u, v, $u - v$ and $u - \lambda v$ are all squares. By Theorem 1.3, $u, v \in K$ so $x, y \in K$. □

Chapter 2

Some Remarks on Plane Cubics

For now, consider a field $K = \bar{K}$ with $\mathrm{char}(K) \neq 2$.

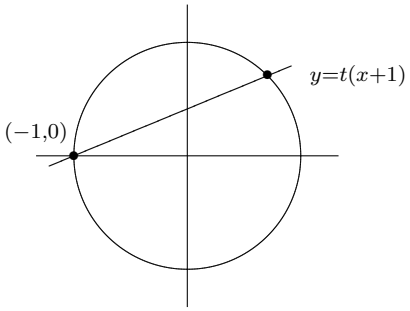
Definition. An algebraic curve C is *rational* if it is birational to $\mathbb{P}^1$.

Example. A plane affine curve $C = \{f(x,y) = 0\} \subset \mathbb{A}^2$ is rational if there exists $\phi, \psi \in K(t)$ such that

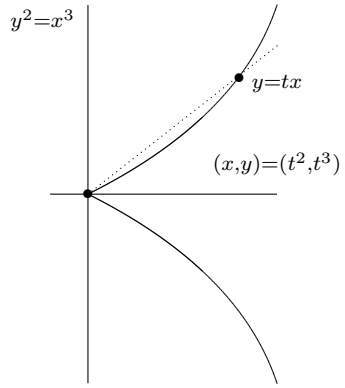
(i) $\mathbb{A}^1 \to \mathbb{A}^2, t \mapsto (\phi(t), \psi(t))$ is injective on $\mathbb{A}^1 - \{\text{finite set}\}$,
(ii) $f(\phi(t), \psi(t)) = 0$.

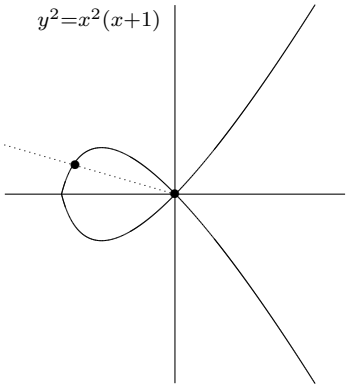
Example.

- Any non-singular conic is rational.



  and $(x,y) = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$.
- Any singular cubic is rational.





By Corollary 1.4, elliptic curves are not rational.

Theorem 2.1. Let $C \subset \mathbb{P}^2$ be a smooth projection cubic. Then we can change coordinates on $\mathbb{P}^2$ such that

$$C\colon Y^2Z = Z^3 f(X/Z)$$

where $f(X) \in K[X]$ is a monic cubic polynomial with distinct roots over $\bar{K}$, i.e., C is an elliptic curve.

Theorem 2.2 (Bezout's Theorem)**.** Plane curves $C, D \subset \mathbb{P}^2$ of degrees m, n with no common components meet in exactly mn points, counted with multiplicity:

$$\sum_{P \in C \cap D} (C.D)_P = mn.$$

Here are some properties of $(C.D)_P$:

(i) $(C.D)_P \geq 1$ if and only if $P \in C \cap D$.
(ii) $(C.D)_P = 1$ if and only of P is a smooth point of C and D, and $T_PC \neq T_PD$.
(iii) If $C = \{F = 0\} \subset \mathbb{P}^2$ and D is the line through P_0 and P_1 then $(C.D)_{P_0} = \operatorname{ord}_{t=0} F(P_0 + tP_1)$.

Definition. $P \in C$ is a *point of inflection*, or *flex*, if $(C.T_PC)_P \geq 3$. For a smooth plane curve $C = \{F = 0\} \subset \mathbb{P}^2$ of degree d, the *Hessian* is $\det H(X_1, X_2, X_3) = \det(\partial^2 F/\partial X_i \partial X_j)_{i,j=1,2,3}$ and has degree $3(d-2)$.

Lemma 2.3. Assume $\operatorname{char}(K) \nmid 2(d-1)$. Then $P \in C$ is a flex if and only if $H(P) = 0$.

Proof. Taylor expand to obtain

$$F(P+X) = F(P) + \sum_i \frac{\partial F}{\partial X_i}(P)X_i + \frac{1}{2}\sum_{i,j} \frac{\partial^2 F}{\partial X_i \partial X_j}(P)X_iX_j + \cdots.$$

The tangent line is

$$T_PC = \Big\{\sum_i \frac{\partial F}{\partial X_i}(P)X_i = 0\Big\}$$

and a conic Q defined by

$$Q = \Big\{\sum_{i,j} \frac{\partial^2 F}{\partial X_i \partial X_j}(P)X_iX_j = 0\Big\}.$$

Then P is a flex if and only if $T_PC \subset Q \implies Q$ is singular if and only if $H(P) = 0$. We claim that P is a smooth point on Q and $T_PQ = T_PC$. Granted the claim, if Q is singular then $T_PC \subset Q$. To show the claim, note that F is homogeneous of degree d so $F(\lambda X) = \lambda^d F(X)$. Taking $\partial/\partial\lambda$ and set $\lambda = 1$,

$$\sum_i X_i \frac{\partial F}{\partial X_i} = dF$$

where $\partial F/\partial X_i$ is homogeneous of degree $d-1$. Repeating this gives

$$\sum_{i,j} X_iX_j \frac{\partial F}{\partial X_i \partial X_j} = d(d-1)F$$

and hence $P \in Q$. We also have

$$T_P Q = \Big\{ \sum_i \Big(\sum_j \frac{\partial^2 F}{\partial X_i \partial X_j}(P) P_j \Big) X_i = 0 \Big\}$$
$$= \Big\{ \sum_i (d-1) \frac{\partial F}{\partial X_i}(P) X_i = 0 \Big\}$$

so that $T_P Q = T_P C$. □

Proof (Theorem 2.1). Let $C = \{F(X,Y,Z) = 0\} \subset \mathbb{P}^2$. By Bezout's Theorem and Lemma 2.3, there exists a flex $P \in C$. Choose coordinates such that $P = (0:1:0)$ and $T_P C = \{Z = 0\}$. As $P \in C$ is a flex, $F(t,1,0) = At^3$ for some constant A, so F has no terms X^2Y, XY^2 or Y^3. Therefore,

$$F \in \langle Y^2 Z, XYZ, YZ^2, X^3, X^2 Z, XZ^2, Z^3 \rangle.$$

Note that the coefficient of $Y^2 Z$ is non-zero (or else $P \in C$ would be singular) and so is the coefficient of X^3 (otherwise C contains the line $Z = 0$). Rescaling X, Y, Z and F, we may assume that

$$C \colon Y^2 Z + a_1 XYZ + a_3 YZ^2 = X^3 + a_2 X^2 Z + a_4 XZ^2 + a_6 Z^3. \qquad (*)$$

Since $\mathrm{char}(K) \neq 2$ we can complete the square, replacing Y by $Y - \frac{1}{2}a_1 X - \frac{1}{2}a_3 Z$, so

$$C \colon Y^2 Z = Z^3 f(X/Z)$$

where f is a monic cubic polynomial. C is smooth so f has distinct roots. (Exercise.) □

Corollary 2.4. Smooth plane cubics are not rational.

Remark. In affine coordinates $x = X/Z$ and $y = Y/Z$, equation $(*)$ becomes

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6,$$

called a Weierstrass equation.

The genus $g(C) \in \mathbb{Z}_{\geq 0}$ is an invariant of a smooth projective curve C.

- If $K = \mathbb{C}$ this is the number of holes in the corresponding Riemann surface.
- If $C \subset \mathbb{P}^2$ is a smooth curve of degree d then $g(C) = (d-1)(d-2)/2$ so for $d \geq 3$, $C \ncong \mathbb{P}^1$.

Let $\phi \colon C_1 \to C_2$ be a non-constant morphism between smooth curves C_1 and C_2. ϕ induces a map $\phi^* \colon K(C_2) \to K(C_1), f \mapsto f \circ \phi$.

Definition. (i) $\deg \phi = [K(C_1) : \phi^* K(C_2)]$.
(ii) ϕ is *separable* if $K(C_1)/\phi^* K(C_2)$ is separable. Note that this is automatic if $\mathrm{char}(K) = 0$.

Theorem 2.5. Let $\phi \colon C_1 \to C_2$ be a non-constant morphism of smooth curves. Then

$$\forall Q \in C_2 \qquad \sum_{P \in \phi^{-1}(Q)} e_\phi(P) = \deg \phi$$

where $e_\phi(P) \in \mathbb{Z}_{\geq 1}$, and if ϕ is separable then $e_\phi(P) = 1$ for all but finitely many $P \in C_1$.

In particular,

(i) ϕ is surjective,
(ii) $|\phi^{-1}(Q)| \leq \deg(\phi)$ for all $Q \in C_2$.

To compute $e_\phi(P)$ take $t \in K(C_2)$ such that $\mathrm{ord}_{\phi(P)}(t) = 1$ and then $e_\phi(P) = \mathrm{ord}_P(\phi^* t)$.

Chapter 3

Weierstrass Equations

Definition. An elliptic curve E/K is a smooth projective curve of genus 1, equipped with a specified K-rational point $\mathcal{O}_E$.

Example. $C = \{X^3 + pY^3 + p^2Z^3 = 0\} \subset \mathbb{P}^2$, p prime. C is a smooth plane cubic over $\mathbb{Q}$, so a curve of genus 1. But C has no $\mathbb{Q}$-rational points, so it is not an elliptic curve.

Theorem 3.1. Every elliptic curve E/K is isomorphic over K to a curve in Weierstrass form via an isomorphism $\mathcal{O}_E \mapsto (0:1:0)$.

Remark. In Chapter 2 we considered the special case $E \subset \mathbb{P}^2$ with $\mathcal{O}_E$ a flex.

Definition. A divisor on E is a finite formal sum of pairs on E, i.e.,

$$D = \sum_{P \in E} n_p.P$$

where $n_p \in \mathbb{Z}$ and $n_p = 0$ for all but finitely many $P \in E$. If $f \in K(E)^*$ then

$$\operatorname{div}(f) = \sum_{P \in E} \operatorname{ord}_P(f).P$$

where $\operatorname{ord}_P(f)$ is the order of vanishing of f at P.

Notation. $D \geq 0$ means $n_P \geq 0$ for all $P \in E$, and $\deg(D) = \sum_{P \in E} n_P \in \mathbb{Z}$.

The *Riemann–Roch space* of D is

$$\mathcal{L}(D) = \{f \in K(E)^* : \operatorname{div}(f) + D \geq 0\} \cup \{0\}.$$

Theorem 3.2 (Riemann–Roch for Genus 1)**.**

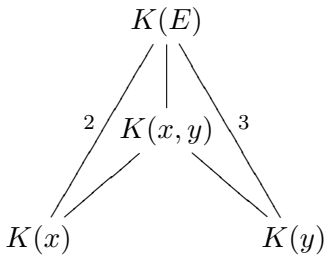
$$\dim \mathcal{L}(D) = \begin{cases} \max\{\deg(D), 0\} & D \neq 0, \\ 1 & D = 0. \end{cases}$$

Proof (Theorem 3.1). Consider $\mathcal{L}(2.\mathcal{O}_E)$ and $\mathcal{L}(3.\mathcal{O}_E)$ and pick bases $1, x$ and $1, x, y$. The 7 elements $1, x, y, x^2, xy, x^3, y^2$ belong to the 6-dimensional space $\mathcal{L}(6.\mathcal{O}_E)$ so satisfy a dependence relation. Those elements have orders $0, 2, 3, 4, 5, 6, 6$, so the coefficients of x^3 and y^2 must be non-zero. Rescaling x and y, we get

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

for some $a_i \in \bar{K}$. In fact, one can show that $a_i \in K$.

We claim that $K(x,y) = K(E)$. Observe that $[K(E) : K(x)] = \deg\big(E \xrightarrow{x} \mathbb{P}^1\big) = -\operatorname{ord}_{\mathcal{O}_E}(x) = 2$ and $[K(E) : K(y)] = \deg\big(E \xrightarrow{y} \mathbb{P}^1\big) = -\operatorname{ord}_{\mathcal{O}_E}(y) = 3$.



By the tower law, $[K(E) : K(x,y)] = 1$. We have the morphism $\phi\colon E \to E', P \mapsto (x(P) : y(P) : 1)$ with

$$\deg \phi = [K(E) : \phi^* K(E')] = [K(E) : K(x,y)] = 1$$

so E and E' are birational. If E' is singular then E and E' are both rational, contradicting that E has genus 1.

It is a fact that a rational map from a smooth curve to a projective variety is automatically a morphism.

Applying this to ϕ^{-1}, it follows that ϕ is an isomorphism

$$\phi\colon E \to E', P \mapsto (x(P) : y(P) : 1) = \left(\frac{x(P)}{y(P)} : 1 : \frac{1}{y(P)}\right), \mathcal{O}_E \mapsto (0 : 1 : 0). \qquad \square$$

Proposition 3.3. Let E and E' be elliptic curves over K in Weierstrass form. Then $E \cong E'$, that is, E and E' are isomorphic via a map sending $\mathcal{O}_E$ to $\mathcal{O}_{E'}$, if and only if they are related by

$$x = u^2 x' + v, \qquad y = u^3 y' + u^2 s x' + t$$

for some $u, v, s, t \in K$ with $u \neq 0$.

Proof. $\langle 1, x\rangle = \mathcal{L}(2.\mathcal{O}_E) = \langle 1, x'\rangle$ so $x = \lambda x' + v$ for some $\lambda, v \in K$ with $\lambda \neq 0$. Also $\langle 1, x, y\rangle = \mathcal{L}(3.\mathcal{O}_E) = \langle 1, x', y'\rangle$ so $y = \mu y' + \sigma x' + t$ for some $\mu, \sigma, t \in K$ with $\mu \neq 0$. Substituting this into the Weierstrass equations and looking at the coefficients of x^3 and y^2, we have $\lambda^3 = \mu^2$ so $\lambda = u^2$, $\mu = u^3$ for some $u = \mu/\lambda \in K$. Set $s = \sigma/u^2$. $\square$

A Weierstrass equation defines an elliptic curve if and only if it defines a smooth plane cubic if and only if $\Delta(a_1, \ldots, a_6) \neq 0$ where Δ is a certain polynomial in $\mathbb{Z}[a_1, \ldots, a_6]$. Note that if $\operatorname{char}(K) \neq 2, 3$ it suffices to consider

$$y^2 = x^3 + ax + b$$

and then $\Delta = -16(4a^3 + 27b^2)$.

Corollary 3.4. Assume that $\operatorname{char}(K) \neq 2, 3$. Then elliptic curves $E\colon y^2 = x^3 + ax + b$ and $E'\colon y^2 = x^3 + a'x + b'$ are isomorphic if and only if

$$a' = u^4 a, \qquad b' = u^6 b$$

for some $u \in K^*$.

Proof. E and E' are related as in Proposition 3.3 with $r = s = t = 0$. □

Definition. The *j-invariant* of E: $y^2 = x^3 + ax + b$ is

$$j(E) = \frac{1728(4a^3)}{4a^3 + 27b^2}.$$

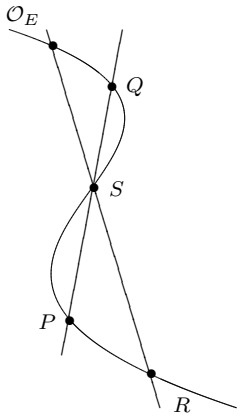
Corollary 3.5. Over $\bar{K}$, $E \cong E'$ if and only if $j(E) = j(E')$.

Proof. $E \cong E'$ if and only if $a' = u^4 a$, $b' = u^6 b$ for some $u \in K^*$ if and only if $(a^3 : b^2) = (a'^3 : b'^2)$ if and only if $j(E) = j(E')$. □

Chapter 4

The Group Law

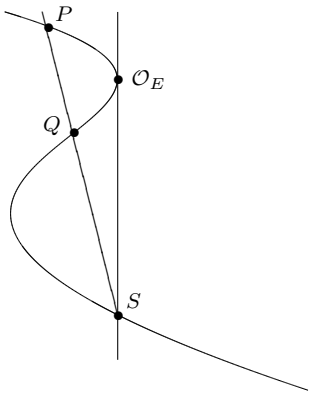
Let $E \subset \mathbb{P}^2$ be a smooth plane cubic with $\mathcal{O}_E \in E$.



By Bezout's Theorem, E meets any line in three points, counted with multiplicity. Let $P, Q \in E$. Let $S = \overline{PQ} \cap E$, let $R = \overline{\mathcal{O}_E S} \cap E$. Define $P \oplus Q = R$. If $P = Q$, take $T_P E$ instead of $\overline{PQ}$ etc. This process is called the *chord-and-tangent process.*

Theorem 4.1. $(E, \oplus)$ is an abelian group.

Proof. (i) $P \oplus Q = Q \oplus P$.
(ii) $\mathcal{O}_E$ is the identity.
(iii) Given P, let $S = T_{\mathcal{O}_E} E \cap E$ and $Q = \overline{PS} \cap E$ then $\ominus P = Q$, i.e., $P \oplus Q = \mathcal{O}_E$.



Note that if $\mathcal{O}_E$ is a flex then $S = \mathcal{O}_E$ in the above.

(iv) Associativity is much harder to prove. □

Now assume that $K = \bar{K}$.

Definition. $D_1, D_2 \in \mathrm{Div}(E)$ are *linearly equivalent* if there exists $f \in K(E)^*$ such that $\mathrm{div}(f) = D_1 - D_2$. Write $D_1 \sim D_2$, and $[D] = \{D' : D' \sim D\}$.

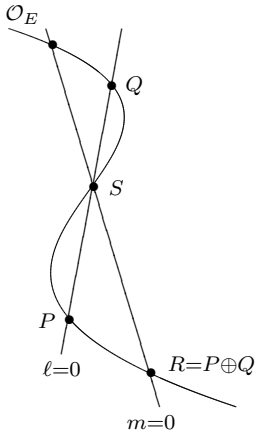
Remark. Theorem 2.5 applied to $f\colon E \to \mathbb{P}^1$ shows $\deg(\mathrm{div}(f)) = 0$, so $D_1 \sim D_2$ implies $\deg(D_1) = \deg(D_2)$.

The principal divisors, i.e., $\mathrm{div}(f)$ for $f \in K(E)^*$ are a subgroup of $\mathrm{Div}(E)$ since $\mathrm{div}(fg) = \mathrm{div}(f) + \mathrm{div}(g)$.

Definition. We define the groups $\mathrm{Pic}(E) = \mathrm{Div}(E)/\sim$ and $\mathrm{Pic}^\circ(E) = \mathrm{Div}^\circ(E)/\sim$ where $\mathrm{Div}^\circ(E) = \{D \in \mathrm{Div}(E) : \deg(D) = 0\}$. For the moment, we also define the map $\phi\colon E \to \mathrm{Pic}^\circ(E), P \mapsto [P - \mathcal{O}_E]$.

Proposition 4.2. (i) $\phi(P \oplus Q) = \phi(P) + \phi(Q)$.
(ii) ϕ is a bijection.

Proof. (i) Consider the lines $l = 0$ and $m = 0$.



Then $l/m \in K(E)^*$ and

$$\begin{aligned}\mathrm{div}\Big(\frac{l}{m}\Big) &= P + S + Q - \mathcal{O}_E - S - R \\ &= P + Q - \mathcal{O}_E - R \\ &= P * Q - \mathcal{O}_E - P \oplus Q\end{aligned}$$

so $P + Q \sim P \oplus Q + \mathcal{O}_E$, hence $P \oplus Q - \mathcal{O}_E \sim P - \mathcal{O}_E + Q - \mathcal{O}_E$ and finally $\phi(P \oplus Q) = \phi(P) + \phi(Q)$.

(ii) (*Injective.*) If $\phi(P) = \phi(Q)$ then $P - Q \sim 0$ so $P \sim Q$. So there exists $f \in K(E)^*$ such that $\mathrm{div}(f) = P - Q$, then $\deg\big(E \xrightarrow{f} \mathbb{P}^1\big) = 1$ and hence $E \cong \mathbb{P}^1$, which contradicts E being an elliptic curve unless f is constant so $P = Q$.
(*Surjective.*) Take $D \in \mathrm{Div}^\circ(E)$. Then $\deg(D + \mathcal{O}_E) = 1$. By Riemann–Roch, $\dim \mathcal{L}(D + \mathcal{O}_E) = 1$ so there exists $f \in K(E)^*$ such that $\mathrm{div}(f) + D + \mathcal{O}_E \geq 0$. The left-hand side also has degree 1. Therefore, $\mathrm{div}(f) + D + \mathcal{O}_E = P$ for some $P \in E$. Then $D + \mathcal{O}_E \sim P$ so $D \sim P - \mathcal{O}_E$ and finally $[D] = [P - \mathcal{O}_E] = \phi(P)$. □

Define sum: $\mathrm{Div}(E) \to E, P_1+\cdots P_r-(Q_1+\cdots+Q_s) \mapsto (P_1 \oplus \cdots \oplus P_r) \ominus (Q_1 \oplus \cdots \oplus Q_s)$. If $D \in \mathrm{Div}^\circ(E)$, say $D = \sum n_i P_i$, then $D = \sum n_i (P_i - \mathcal{O}_E)$ so

$$[D] = \sum n_i [P_i - \mathcal{O}_E] = \sum n_i \phi(P_i) = \phi(\mathrm{sum}(D))$$

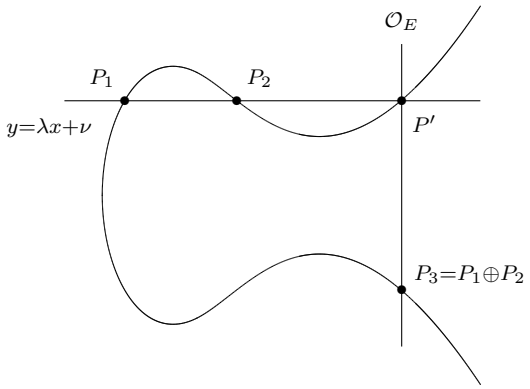
by Proposition 4.2 (i). So $D \sim 0$ if and only if $\mathrm{sum}(D) = \mathcal{O}_E$.

Corollary 4.3. If $D \in \mathrm{Div}(E)$ then $D \sim \mathcal{O}_E$, i.e., D is principal, if and only if $\deg(D) = 0$ and $\mathrm{sum}(D) = \mathcal{O}_E$.

4.1 Formlae for E in Weierstrass Form

We consider an elliptic curve with general Weierstrass equation

$$E\colon y^2 = a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \qquad (*)$$



The inverse of (x, y) is $(x, -(a_1x + a_3) - y)$. Substituting $y = \lambda x + \nu$ into $(*)$ and taking coefficients of x^2 gives $\lambda^2 + a_1\lambda - a_2 = x_1 + x_2 + x' = x_1 + x_2 + x_3$ so

$$\begin{aligned} x_3 &= \lambda^2 + a_1\lambda - a_2 - x_1 - x_2, \\ y' &= \lambda x' + \nu, \\ y_3 &= -(a_1x_3 + a_3) - \lambda x_3 - \nu = -(a_1 + \lambda)x_3 + a_3 - \nu. \end{aligned}$$

It remains to give formulae for λ and ν.

Case 1. $x_1 = x_2$, $P_1 \neq P_2$. Then $P_1 \oplus P_2 = \mathcal{O}_E$.

Case 2. $x_1 \neq x_2$. Then

$$\lambda = \frac{y_1 - y_2}{x_1 - x_2}, \qquad \nu = y_1 - \lambda x_1 = \frac{x_1y_2 - x_2y_1}{x_1 - x_2}.$$

Case 3. $P_1 = P_2$. Use the tangent line, see formula sheet.

Theorem 4.4. Elliptic curves are group varieties, i.e., the group operations

$$[-1]\colon E \to E, P \mapsto \ominus P, \qquad \oplus\colon E \times E \to E$$

are morphisms of algebraic varieties.

Proof. (i) $[-1]\colon E \to E$ is a rational map and hence a morphism.

(ii) We need to show that $\oplus$ is a morphism. The formulae in Case 2 show it is a rational map regular on $U = \{(P,Q) : P, Q, P \oplus Q, P \ominus Q \neq \mathcal{O}_E\}$. Fix $P \in E$ and define the translation $\tau_P \colon E \to E, X \mapsto P \oplus X$. Note that τ_P is rational so a morphism. We can factor $\oplus$ as

$$E \times E \xrightarrow{\tau_A \times \tau_B} E \times E \xrightarrow{\oplus} E \xrightarrow{\tau_{\ominus A \ominus B}} E$$

for any $A, B \in E$. So $\oplus$ is regular on all translations of U, and these cover all of $E \times E$. Thus $\oplus$ is a morphism. □

Let K be any field and E an elliptic curve over K. Set

$$E(K) = \{(x,y) \in K^2 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{\mathcal{O}_E\}.$$

Lemma 4.5. $(E(K), \oplus)$ is an abelian group.

4.2 Statement of Results

(i) $K = \mathbb{C}$, $E(\mathbb{C}) \cong C/\Lambda \cong \mathbb{R}/\mathbb{Z} \times \mathbb{R}/\mathbb{Z}$, where Λ is a rank 2 lattice, and the isomorphisms are isomorphims of topological groups.

To add further brief remarks, note that the meromorphic functions on $\mathbb{C}/\Lambda$ correspond precisely to the Λ-invariant meromorphic functions on $\mathbb{C}$. The function field $\mathbb{C}/\Lambda$ is generated by $\wp(z)$ and $\wp'(z)$ where $\wp$ is the Weierstrass function. One shows that $\mathbb{C}/\Lambda \cong E(\mathbb{C})$ for some elliptic curve $E/\mathbb{C}$. The Uniformisation Theorem gives that every elliptic curve $E/\mathbb{C}$ arises this way.

(ii) $K = \mathbb{R}$,

$$E(\mathbb{R}) = \begin{cases} \mathbb{Z}/2\mathbb{Z} \times \mathbb{R}/\mathbb{Z} & \Delta > 0, \\ \mathbb{R}/\mathbb{Z} & \Delta < 0. \end{cases}$$

(iii) $K = \mathbb{F}_q$, $|\#E(\mathbb{F}_q) - (q+1)| \leq 2\sqrt{q}$, which is Hasse's Theorem.

(iv) $[K : \mathbb{Q}_p] < \infty$, $\mathcal{O}_K$ the ring of integers. Then $E(K)$ contains a subgroup of finite index isomorphic to $(\mathcal{O}_K, +)$.

(v) $[K : \mathbb{Q}] < \infty$, $E(K)$ is a finitely generated abelian group, which is the Mordell–Weil Theorem. From basic group theory, we know that if A is a finitely generated group then $A \cong F \times \mathbb{Z}^r$ where F is a finite group and r is the rank of A. If K is a number field then proof of the Mordell–Weil Theorem gives an upper bound for rank(E). But there is no algorithm proven to compute the rank in all cases.

Chapter 5

Isogenies

For now assume that $K = \bar{K}$ and write $E = E(\bar{K})$.

Definition. Let E_1 and E_2 be elliptic curves over K.

(i) An *isogeny* $\phi\colon E_1 \to E_2$ is a non-constant morphism with $\phi(\mathcal{O}_{E_1}) = \mathcal{O}_{E_2}$. We recall that a non-constant morphism is surjective.
(ii) E_1 and E_2 are *isogenous* if there exists an isogeny $E_1 \to E_2$.

Remark. If $E_1 \xrightarrow{\phi} E_2 \xrightarrow{\psi} E_3$ are isogenies then ϕ and ψ are surjective and so $\psi \circ \phi\colon E_1 \to E_3$ is an isogeny. By the tower law, $\deg(\psi \circ \phi) = \deg(\psi)\deg(\phi)$. For $n \in \mathbb{Z}$ let $[n]\colon E \to E, P \mapsto P \oplus \cdots \oplus P$. If $n < 0$ then $[n] = [-1] \circ [-n]$.

Remark. $E[n] = \ker\big(E \xrightarrow{[n]} E\big)$ is the n-torsion of E.

Lemma 5.1. Assume $\mathrm{char}(K) \neq 2$, $E\colon y^2 = f(x) = (x - e_1)(x - e_2)(x - e_3)$. Then

$$E[2] = \{\mathcal{O}_E, (e_1, 0), (e_2, 0), (e_3, 0)\} \cong (\mathbb{Z}/2\mathbb{Z})^2.$$

Proof. Let $\mathcal{O}_E \neq P \in E$ and write $P = (x_P, y_P)$. Then $T_P E = \{f'(x_P)(x - x_P) = 2y_P(y - y_P)\}$ and $P \in E[2]$ if and only if $P \oplus P = \mathcal{O}_E$ if and only if $T_P E = \{x = x_P\}$ if and only if $y_P = 0$. □

Lemma 5.2. Let $n \in \mathbb{Z}, n \neq 0$. Then $[n] \neq [0]$ so $[n]$ is an isogeny.

Proof. Assume $\mathrm{char}(K) \neq 2$. *Case* $n = 2$. Lemma 5.1 gives $E[2] \neq E$ so $[2] \neq [0]$. *Case* n *odd.* Lemma 5.1 gives that there exists $\mathcal{O}_E \neq T \in E[2]$. n is odd so $[n]T = T \neq \mathcal{O}_E$. Therefore, $[n] \neq [0]$. Now use that $[mn] = [m] \circ [n]$.

If $\mathrm{char}(K) = 2$, we can use a similar result on 3-torsion points. □

Theorem 5.3. If $\phi\colon E_1 \to E_2$ is an isogeny then $\phi(P \oplus Q) = \phi(P) \oplus \phi(Q)$.

Sketch of proof. ϕ induces $\phi_*\colon \mathrm{Div}(E_1) \to \mathrm{Div}(E_2), \sum n_P P \mapsto \sum n_P \phi(P)$. Recall that $\phi^*\colon K(E_2) \hookrightarrow K(E_1)$ is a field extension,

$$\begin{array}{c} K(E_1) \\ \big| \quad \big) \text{ norm map} \\ K(E_2) \end{array}$$

It is a fact that if $f \in K(E_1)^*$ then $\operatorname{div}\big(N_{K(E_1)/K(E_2)}(f)\big) = \phi_*(\operatorname{div}(f))$, i.e., ϕ_* maps principal divisors to principal divisors. Also $\phi(\mathcal{O}_{E_1}) = \mathcal{O}_{E_2}$ so we have a commutative diagram

$$\begin{array}{ccccc} P & & E_1 & \xrightarrow{\phi} & E_2 & & Q \\ \downarrow & & \cong\downarrow & & \downarrow\cong & & \downarrow \\ [P - \mathcal{O}_{E_1}] & & \operatorname{Pic}^\circ(E_1) & \xrightarrow{\phi_*} & \operatorname{Pic}^\circ(E_2) & & [Q - \mathcal{O}_{E_2}] \end{array}$$

ϕ_* is a group homomorphism, so ϕ is a homomorphism. □

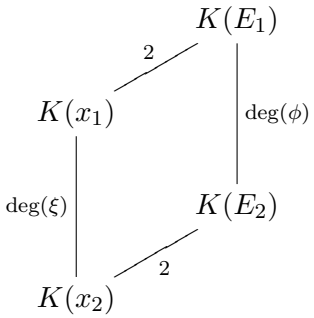
5.1 Computing Degrees of Isogenies

Lemma 5.4. If $\phi\colon E_1 \to E_2$ is an isogeny then there exists a morphism ξ such that the diagram

$$\begin{array}{ccc} E_1 & \xrightarrow{\phi} & E_2 \\ {\scriptstyle x_1}\downarrow & & \downarrow{\scriptstyle x_2} \\ \mathbb{P}^1 & \xrightarrow{\xi} & \mathbb{P}^1 \end{array}$$

commutes, where x_i is the x-coordinate for a Weierstrass equations. Moreover, writing $\xi(X) = r(X)/s(X)$ with $r, s \in K[X]$ coprime, we have $\deg(\phi) = \max\{\deg(r), \deg(s)\}$.

Proof. For $i = 1, 2$, $K(E_i)$ is a degree 2 Galois extension of $K(x_i)$ with Galois group generated by $[-1]^*$. By Theorem 5.3, $\phi \circ [-1] = [-1] \circ \phi$. If $f \in K(x_2)$ then $[-1]^*(\phi^* f) = \phi^*([-1]^* f) = \phi^*(f)$ so $\phi * (f) \in K(x_1)$.



We have identified $K(x_2)$ as a subfield of $K(x_1)$ via $x_2 = \xi(x_1) = r(x_1)/s(x_1)$. x_1 is a root of $F(X) = r(X) - x_2 s(X) \in K(x_2)[X]$. Now $\gcd(r(X), s(X)) = 1$ and $F(X)$ is irreducible in $K[x_2, X]$ so by Gauss' Lemma $F(X)$ is irreducible in $K(x_2)[X]$. So $F(X)$ is the minimal polynomial of x_1 over $K(x_2)$. Therefore, $\deg(\xi) = \deg(F) = \max\{\deg(r), \deg(s)\}$. □

Lemma 5.5.

$$\deg[2] = 4.$$

Proof. Assume for simplicity that $\operatorname{char}(K) \neq 2, 3$ so that $E\colon y^2 = x^3 + ax + b$. Then

$$[2]\colon E \to E, (x, y) \mapsto \left(\left(\frac{3x^2 + a}{2y}\right)^2 - 2x, *\right)$$

so

$$\xi(x) = \frac{(3x^2+a)^2 - 8x(x^3+ax+b)}{4(x^3+ax+b)}$$

and note that the numerator and denominator are coprime, for otherwise a common root θ would give $(\theta, 0)$ as a singular point on E, a contradiction. Thus $\deg[2] = \deg(\xi) = 4$. □

For isogenies $\phi, \psi\colon E_1 \to E_2$ define $\phi + \psi\colon E_1 \to E_2, P \mapsto \phi(P) \oplus \psi(P)$.

Lemma 5.6. Let $\phi, \psi\colon E_1 \to E_2$ be isogenies and assume that ψ, ϕ, $\phi+\psi$ and $\phi-\psi$ are not the zero map. Then

$$\deg(\phi+\psi) + \deg(\phi-\psi) \leq 2\deg(\phi) + 2\deg(\psi).$$

Proof. For simplicity, assume that $\mathrm{char}(K) \neq 2, 3$. Let $E_2\colon y^2 : x^3 + ax + b$ and write

$$\begin{aligned} \phi\colon (x,y) &\mapsto (\xi_1(x), \eta_1(x,y)) & \psi\colon (x,y) &\mapsto (\xi_2(x), \eta_2(x,y)) \\ \phi+\psi\colon (x,y) &\mapsto (\xi_3(x), \eta_3(x,y)) & \phi-\psi\colon (x,y) &\mapsto (\xi_4(x), \eta_4(x,y)) \end{aligned}$$

Explicit calculations as shown on the formulae sheet show that $\xi_3 + \xi_4$ and $\xi_3\xi_4$ are polynomials in ξ_1 and ξ_2. Setting $\xi_i = r_i/s_i$ with $r_i, s_i \in K[X]$ coprime. Then

$$(1 : \xi_3 + \xi_4 : \xi_3\xi_4) = (s_3s_4 : r_3s_4 + r_4s_3 : r_3r_4) = (w_0 : w_1 : w_2)$$

where

$$\begin{aligned} w_0 &= (r_1s_2 - r_2s_1)^2, \\ w_1 &= 2(r_1r_2 + as_1s_2)(r_1s_2 + r_2s_1) + 4bs_1^2s_2^2, \\ w_2 &= r_1^2r_2^2 - 2ar_1r_2s_1s_2 - 4bs_1s_2(r_1s_2 + r_2s_1) + a^2s_1^2s_2^2. \end{aligned}$$

As $\gcd(r_i, s_i) = 1$ we have that $\gcd(s_3s_4, r_3s_4 + r_4s_3, r_3r_4) = 1$, so

$$\begin{aligned} \deg(\xi_3) + \deg(\xi_4) &= \max\{\deg(r_3), \deg(s_3)\} + \max\{\deg(r_4), \deg(s_4)\} \\ &= \max\{\deg(s_3s_4), \deg(r_3s_4 + r_4s_3), \deg(r_3r_4)\} \\ &\leq \max\{\deg(w_i) : i = 0, 1, 2\} \\ &\leq 2\max\{\deg(r_1), \deg(s_1)\} + 2\max\{\deg(r_2), \deg(s_2)\} \\ &= 2\deg(\xi_1) + 2\deg(\xi_2). \end{aligned}$$

By Lemma 5.4, the result follows. □

Recall that over $K = \mathbb{C}$, $E \cong \mathbb{C}/\Lambda \cong \mathbb{R}/\mathbb{Z} \times \mathbb{R}/\mathbb{Z}$. It follows that

(i) $E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$,
(ii) $\deg[n] = n^2$.

We shall show that (ii) holds for all K and (i) holds if $\mathrm{char}(K) \nmid n$.

Notation. Let E_1 and E_2 be elliptic curves over K. Then $\mathrm{Hom}(E_1, E_2)$ is the space of isogenies $E_1 \to E_2$ and the zero map. It is an abelian group under $(\phi+\psi)(P) = \phi(P) \oplus \psi(P)$. By convention, $\deg(0) = 0$.

Theorem 5.7. The map deg: $\mathrm{Hom}(E_1, E_2) \to \mathbb{Z}$ is a positive-definite quadratic form, that is,

(i) $\deg(n\phi) = n^2 \deg(\phi)$,
(ii) $(\phi, \psi) \mapsto \deg(\phi + \psi) - \deg(\phi) - \deg(\psi)$ is $\mathbb{Z}$-bilinear,
(iii) $\deg(\phi) \geq 0$ with equality if and only if $\phi = 0$.

We observe that (iii) is clear since any isogeny has degree at least 1.

Lemma 5.8. Let $\phi, \psi \in \mathrm{Hom}(E_1, E_2)$. Then

$$\deg(\phi + \psi) + \deg(\phi - \psi) = 2\deg(\phi) + 2\deg(\psi).$$

Proof. The $\leq$ direction follows from Lemma 5.6 if ϕ, ψ, $\phi + \psi$ and $\phi - \psi$ are non-zero. If ϕ or ψ is zero the result is clear. If $\phi = \pm\psi$ we use that

$$\deg(2\phi) = \deg[2]\deg(\phi) = 4\deg(\phi)$$

by Lemma 5.5. For the $\geq$ direction, replace ϕ and ψ by $\phi + \psi$ and $\phi - \psi$ to get

$$\deg(2\phi) + \deg(2\psi) \leq 2\deg(\phi + \psi) + 2\deg(\phi - \psi)$$

which is the reverse inequality. □

Lemma 5.9.

$$\deg[n] = n^2.$$

Proof. By induction on n. The cases $n = 0, 1$ are clear. Apply Lemma 5.8 to the maps $\phi = [n]$ and $\psi = [1]$ to find

$$\deg[n+1] + \deg[n-1] = 2\deg[n] + 2$$

and by hypothesis, $\deg[n+1] = 2n^2 + 2 - (n-1)^2 = (n+1)^2$. If $n < 0$ then $[n] = [-1] \circ [-n]$ so $\deg[n] = \deg[-1]\deg[-n] = n^2$. □

We still need to show that $\langle \phi, \psi \rangle = \deg(\phi + \psi) - \deg(\phi) - \deg(\psi)$ is $\mathbb{Z}$-bilinear, i.e., $\langle \phi_1 + \phi_2, \psi \rangle = \langle \phi_1, \psi \rangle + \langle \phi_2, \psi \rangle$, i.e.,

$$\deg(\phi_1 + \phi_2 + \phi_3) = \deg(\phi_1 + \phi_2) + \deg(\phi_2 + \phi_3) + \deg(\phi_3 + \phi_1) + \deg(\phi_1) + \deg(\phi_2) + \deg(\phi_3).$$

This follows from Lemma 5.8. (Exercise.)

Chapter 6

The Invariant Differential

Let C be a smooth projective curve over K and assume $K = \bar{K}$. The space of differential Ω_c is is the $K(C)$-vector space generated by the symbols dx for $x \in K(C)$ subject to

(i) $\forall x, y \in K(C) \quad d(x+y) = dx + dy$,
(ii) $\forall x, y \in K(C) \quad d(xy) = xdy + ydx$,
(iii) $\forall a \in K \quad da = 0$.

Fact. Ω_c is a 1-dimensional $K(C)$-vector space.

Let $\omega \in \Omega_c$ and $P \in C$. Take a uniformiser $t \in K(C)$ at P so $\mathrm{ord}_P(t) = 1$. Then $\omega = fdt$ for some $f \in K(C)$. Define $\mathrm{ord}_P(\omega) = \mathrm{ord}_P(t)$.

Fact. (i) This is independent of the choice of t.
(ii) $\mathrm{ord}_P(\omega) = 0$ at all but finitely many $P \in C$.
(iii) If $x \in K(C)$ such that $\mathrm{ord}_P(x) = n \neq 0$ and if $\mathrm{char}(K) \nmid n$ then $\mathrm{ord}_P(dx) = n - 1$.

Definition.

$$\mathrm{div}(\omega) = \sum_{P \in C} \mathrm{ord}_P(\omega).P.$$

Definition. ω is *regular* if $\mathrm{div}(\omega) \geq 0$.

Definition. The *genus* of C is $g(C) = \dim_K\{\omega \in \Omega_c : \mathrm{div}(\omega) \geq 0\}$. By Riemann–Roch,

$$\forall \omega \in \Omega_c - \{0\} \quad \deg(\mathrm{div}(\omega)) = 2g(C) - 2.$$

Lemma 6.1. Assume $\mathrm{char}(K) \neq 2$ and consider $E\colon y^2 = (x-e_1)(x-e_2)(x-e_3)$. Then $\omega = (dx)/y$ is a differential on E with no poles or zeros. Hence $g(C) = 1$.

Proof. Let $T_i = (e_i, 0)$. So $E[2] = \{\mathcal{O}_E, T_1, T_2, T_3\}$. Then $\mathrm{div}(y) = T_1 + T_2 + T_3 - 3.\mathcal{O}_E$. If $P \in E \setminus E[2]$ then

$$\mathrm{ord}_P(x - x_P) = 1 \quad \Longrightarrow \quad \mathrm{ord}_P(dx) = 0.$$

If $P = T_i$ then

$$\mathrm{ord}_P(x - e_i) = 2 \quad \Longrightarrow \quad \mathrm{ord}_P(dx) = 1.$$

If $P = \mathcal{O}_E$ then

$$\mathrm{ord}_P(x) = -2 \quad \Longrightarrow \quad \mathrm{ord}_P(dx) = -3.$$

Hence $\mathrm{div}(dx) = T_1 + T_2 + T_3 - 3.\mathcal{O}_E$ and $\mathrm{div}(\omega) = \mathrm{div}(dx) - \mathrm{div}(y) = 0$. □

Let $\phi\colon C_1 \to C_2$ be a non-constant morphism of smooth projective curves. This induces $\phi^*\colon \Omega_{C_2} \to \Omega_{C_1}, fdg \mapsto \phi^* f d(\phi^* g)$.

Lemma 6.2. ϕ is separable if and only if $\phi^*\colon \Omega_{C_2} \to \Omega_{C_1}$ is non-zero.

Proof. Omitted. □

Lemma 6.3. Let E/K be an elliptic curve and ω a non-zero regular differential on E. Then $\tau_P^*\omega = \omega$ for all $P \in E$. Recall that $\tau_P\colon E \to E, Q \mapsto P \oplus Q$. ω is called the *invariant differential*.

Proof. As $g(E) = 1$, every regular differential is a scalar multiple of ω. Therefore, $\tau_P^*\omega = \lambda_P\omega$ for some $\lambda_P \in K^*$. The morphism $E \to \mathbb{P}^1, P \mapsto \lambda_P$ is not surjective, it misses 0 and ∞, hence it is constant. Hence $\tau_P^* w = \lambda$ for some $\lambda \in K^*$. Finally, taking $P = \mathcal{O}_E$ gives $\lambda = 1$. □

Lemma 6.4. Let $\phi, \psi\colon E_1 \to E_2$ are isogenies and ω be the invariant differential on E_2. Then $(\phi + \psi)^*\omega = \phi^*\omega + \psi^*\omega$.

Proof. Define maps $\mu\colon E_2 \times E_2 \to E_2, (P, Q) \mapsto P \oplus Q$, $\pi_1\colon (P, Q) \mapsto P$ and $\pi_2\colon (P, Q) \mapsto Q$.

It is a fact that $\Omega_{E_2 \times E_2}$ is a 2-dimensional vector space over $K(E_2 \times E_2)$ with basis $\pi_1^*\omega$ and $\pi_2^*\omega$. Therefore,

$$\mu^*\omega = f\pi_1^*\omega + g\pi_2^*\omega \tag{$*$}$$

for some $f, g \in K(E_2 \times E_2)$. If $\iota\colon C \to E_2 \times E_2$ is a morphism, pull back $(*)$ by ι,

$$(\mu \circ \iota)^*\omega = (\iota^* f)(\pi_1 \circ \iota)^*\omega + (\iota^* g)(\pi_2 \circ \iota)^*\omega. \tag{$**$}$$

Fix $Q \in E_2$, let $\iota\colon E_2 \to E_2 \times E_2, P \mapsto (P, Q)$. Then

$$\tau_Q^*\omega = (\iota^* f)\omega + Q.$$

By Lemma 6.3, $\iota^* f = 1$ so $(P \mapsto f(P, Q)) = 1$ and $f(P, Q) = 1$ for all $P \in E_2$. Therefore, $f = 1$ and by symmetry $g = 1$. Now take $\iota\colon E_1 \to E_2 \times E_2, P \mapsto (\phi(P), \psi(P))$. Then $(**)$ says

$$(\phi + \psi)^*\omega = \phi^*\omega + \psi^*\omega.$$

□

Example. Consider $G_m = \mathbb{A}^1 - \{0\}$, the multiplicative group. $\phi\colon G_m \to G_m, x \mapsto x^n$. Then $\phi^*(dx) = d(x^n) = nx^{n-1}dx$. If $\mathrm{char}(K) \nmid n$, by Lemma 6.2 ϕ^* is separable and so by Theorem 2.5, $|\phi^{-1}(Q)| \leq \deg\phi = n$, with equality for all but finitely many $Q \in G_m$.

Theorem 6.5. Let E/K be an elliptic curve, $\mathrm{char}(K) \nmid n$. Then $E[n] = (\mathbb{Z}/n\mathbb{Z})^2$.

Proof. Let ω be the invariant differential on E. Lemma 6.4 and induction give $[n]^*\omega = n\omega \neq 0$ as $\mathrm{char}(K) \nmid n$. Hence $[n]\colon E \to E$ is separable. By Theorem 2.5 and Lemma 5.9, $|[n]^{-1}(Q)| \leq \deg[n] = n^2$ with equality for all but finitely many $Q \in E$. But $[n]$ is a group homomorphism, so $|E[n]| = n^2$. The classification of finite abelian groups gives that $E[n] \cong \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_t\mathbb{Z}$ with $d_1 \mid \cdots \mid d_t \mid n$. If p is a prime divisor of d_1 then $E[p] \cong (\mathbb{Z}/p\mathbb{Z})^t$. From $|E[n]| = n^2$ with $n = p$ we conclude that $t = 2$ and so $E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$. □

Remark. If $p = \mathrm{char}(K)$ then $E[p]$ is 0 or $\mathbb{Z}/p\mathbb{Z}$, called the super-singular and ordinary cases, respectively.

Theorem 6.6 (Hasse)**.** Let $E/\mathbb{F}_q$ be an elliptic curve. Then

$$|\#E(\mathbb{F}_q) - (q+1)| \leq 2\sqrt{q}.$$

Lemma 6.7. Suppose A is an abelian group and $q\colon A \to \mathbb{Z}$ a positive definite quadratic form. If $\phi, \psi \in A$ then

$$|q(\phi+\psi) - q(\phi) - q(\psi)| \leq 2\sqrt{q(\phi)q(\psi)}.$$

Proof. Let $\langle \phi, \psi \rangle = q(\phi+\psi) - q(\phi) - q(\psi)$. Then for all $m, n \in \mathbb{Z}$ we have

$$\langle m\phi + n\psi, m\phi + n\psi \rangle = m^2\langle \phi, \phi \rangle + 2mn\langle \phi, \psi \rangle + n^2\langle \psi, \psi \rangle$$

and hence

$$q(m\phi + n\psi) = m^2 q(\phi) + mn\langle \phi, \psi \rangle + n^2 q(\psi) \geq 0$$

so, for all $t \in \mathbb{Q}$,

$$q(\phi)t^2 + \langle \phi, \psi \rangle t + q(\psi) \geq 0.$$

This is a quadratic in t and it has at most one real root, hence the discriminant is non-positive, so

$$|\langle \phi, \psi \rangle|^2 \leq 4q(\phi)q(\psi). \qquad \square$$

Proof (Theorem 6.6). If $x \in \bar{\mathbb{F}}_q$ then by Galois Theory, $x \in \mathbb{F}_q$ if and only if $x^q = x$. Define $\phi\colon E \to E, (x, y) \mapsto (x^q, y^q)$ and note ϕ is an isogeny as E is defined over $\mathbb{F}_q$.

$$E(\mathbb{F}_q) = \{P \in E : \phi(P) = P\} = \ker(\phi - 1)$$

If $\omega = (dx)/y$ then

$$\phi^*\omega = \frac{d(x^q)}{y^q} = \frac{qx^{q-1}dx}{y^q} = 0.$$

Thus $(\phi - 1)^*\omega = \phi^*\omega + [-1]^*\omega = -\omega \neq 0$, so $\phi - 1$ is separable, so $|E(\mathbb{F}_q)| = |\ker(\phi - 1)| = \deg(\phi - 1)$. Applying Lemma 6.7 to $\deg\colon \mathrm{Hom}(E, E) \to \mathbb{Z}$ and $\psi = [-1]$,

$$|\deg(\phi - 1) - 1 - \deg(\phi)| \leq 2\sqrt{\deg(\phi)}$$

and note that $\deg(\phi) = q$ by Lemma 5.4. $\square$

Chapter 7

Formal Groups

Consider an elliptic curve of the general form

$$E\colon Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \qquad (*)$$

with $\mathcal{O}_E = (0:1:0)$. The usual affine piece is obtained by taking $x = X/Z$ and $y = Y/Z$. Another affine piece can be obtained via $t = -X/Y$ and $w = -Z/Y$, giving

$$w = t^3 + a_1tw + a_2t^2w + a_3w^2 + a_4tw^2 + a_6w^3 = f(t,w).$$

Our first aim is to find a power series $w = w(t)$ such that $w(t) = f(t, w(t))$, where $w(t) \in \mathbb{Z}[a_1, \ldots, a_6][[t]]$.

Let R be a ring and $I \leq R$ an ideal. The *I-adic topology* on R has basis

$$\{r + I^n : r \in R, n \geq 0\}.$$

Definition. R is *complete* if $\bigcap_{n\geq 0} I^n = \{0\}$ and every Cauchy sequence converges.

Remark. If $x \in I$ then $1 + x \in R^\times$ since $(1+x)^{-1} = 1 - x + x^2 - x^3 + \cdots$ and now assume that R is complete.

Lemma 7.1. Suppose R is complete with respect to an ideal I, $F(X) \in R[X]$ is a polynomial and $s \geq 1$ an integer. If $a \in R$ such that $F(a) \equiv 0 \pmod{I^s}$ and $F'(a) \in R^\times$ then there exists $b \in R$ such that $F(b) = 0$, $b \equiv a \pmod{I^s}$. Moreover, if R is an integral domain then b is unique.

Proof. Let $\alpha \in R^\times$ be such that $F'(a) \equiv \alpha \pmod{I}$. Replacing $F(X)$ by $F(X+a)/\alpha$, we may assume that $F(0) \equiv 0 \pmod{I^s}$ and $F'(0) \equiv 1 \pmod{I}$. We construct a sequence in R satisfying

$$x_0 = 0, \qquad x_{n+1} = x_n - F(x_n). \qquad (*)$$

Then by induction,

$$x_n \equiv 0 \pmod{I^s} \qquad (**)$$

for all $n \geq 0$.

We claim that $x_{n+1} \equiv x_n \pmod{I^{n+s}}$ for all $n \geq 0$. This is shown by induction on n. The case $n = 0$ is clear and we now use the identity

$$F(X) - F(Y) = (X - Y)(F'(0) + \mathcal{O}(X, Y)). \qquad (\dagger)$$

Then, by hypothesis, $x_n \equiv x_{n-1} \pmod{I^{n+s-1}}$ so $F(x_n) - F(x_{n-1}) \equiv x_n - x_{n-1} \pmod{I^{n+s}}$, so $x_{n+1} \equiv x_n \pmod{I^{n+s}}$. This proves the claim.

So (x_n) is Cauchy. As R is complete, $x_n \to b$ as $n \to \infty$ for some $b \in R$. Considering the limit as $n \to \infty$ in $(*)$ shows that $F(b) = 0$, and likewise $(**)$ gives $b \equiv 0 \pmod{I^s}$. Finally, if R is an integral domain then uniqueness follows from $(\dagger)$. □

Now take $R = \mathbb{Z}[a_1, \ldots, a_6][[t]]$ and $I = (t)$, noting that R is complete. Apply Lemma 7.1 with $F(X) = X - f(t, X)$, $a = 0$ and $s = 3$. Then $F'(0) \equiv 1 \pmod{I}$ and we get $w(t) \in \mathbb{Z}[a_1, \ldots, a_6][[t]]$ such that $w(t) = f(t, w(t))$, i.e., $(t, w(t)) \in E$. In fact, $w(t) = t^3(1 + A_1 t + A_2 t^2 + \cdots)$ where $A_1 a_1$, $A_2 = a_1^2 + a_2$, $A_3 = a_1^3 + 2a_1 a_2 + a_3$ etc.

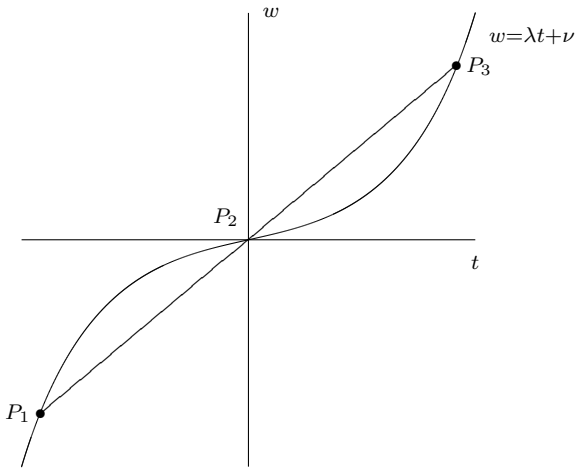
Proposition 7.2. (i) There exists a power series $\iota(t) \in \mathbb{Z}[a_1, \ldots, a_6][[t]]$ such that

$$[-1](t, w(t)) = (\iota(t), w(\iota(t))).$$

(ii) There exists a power series $F(t_1, t_2) \in \mathbb{Z}[a_1, \ldots, a_6][[t_1, t_2]]$ such that

$$(t_1, w(t_1)) \oplus (t_2, w(t_2)) = (F(t_1, t_2), w(F(t_1, t_2))).$$

Proof. With the same notation as above,



where $w_i = w(t_i)$ for $i = 1, 2$ and

$$\lambda = \frac{w_2 - w_1}{t_2 - t_1} = \sum_{n=3}^{\infty} A_{n-3} \frac{t_2^n - t_1^n}{t_2 - t_1} \in \mathbb{Z}[a_1, \ldots, a_6][[t_1, t_2]],$$
$$\nu = w_1 - \lambda t_1 \in \mathbb{Z}[a_1, \ldots, a_6][[t_1, t_2]].$$

Substituting $w = \lambda t + \nu$ into $w = f(t, w)$ we find that

$$\lambda t + \nu = t^3 + a_1 t(\lambda t + \nu) + a_2 t^2(\lambda t + \nu) + a_3(\lambda t + \nu)^2 + a_4 t(\lambda t + \nu)^2 + a_6(\lambda t + \nu)^3.$$

Let A be the coefficient of t^3, so $A = 1 + a_2\lambda + a_4\lambda^2 + a_6\lambda^3$, and let B be the coefficient of t^2, so $B = a_1\lambda + a_2\nu + a_3\lambda^2 + 2a_4\lambda\nu + 3a_6\lambda^2\nu$. Hence $t_1 + t_2 + t_3 = -B/A \in \mathbb{Z}[a_1, \ldots, a_6][[t_1, t_2]]$. Note that $A \equiv 1 \pmod{t_1, t_2}$, so A is a unit.

We have constructed $t_3 = t_3(t_1, t_2) \in \mathbb{Z}[a_1, \ldots, a_6][[t_1, t_2]]$, and put $w_3 = \lambda t_3 + \nu \in \mathbb{Z}[a_1, \ldots, a_6][[t_1, t_2]]$ so that $(t_3, w_3) \in E$. Uniqueness in Lemma 7.1 gives that $w_3 = w(t_3)$.

Now put (i) $t_1 = t$, $t_2 = 0$ so $t_3 = \iota(t)$, and (ii) $F(t_1, t_2) = \iota(t_3)$. □

Here are some properties of F:

(i) $F(X,Y) = F(Y,X)$,
(ii) $F(X,0) = X$ and $F(0,Y) = Y$,
(iii) $F(F(X,Y),Z) = F(X,F(Y,Z))$,
(iv) $F(X,\iota(X)) = 0$.

These are inherited from the group law on E.

Definition. A *formal group* $\mathcal{F}$ over a ring R is a power series $F(X,Y) \in R[[X,Y]]$ such that

(i) $F(X,Y) = F(Y,X)$,
(ii) $F(X,0) = X$ and $F(0,Y) = Y$,
(iii) $F(X,F(Y,Z)) = F(F(X,Y),Z)$.

Remark. We can show that there exists a power series $\iota(T) \in R[[T]]$ such that $F(X,\iota(X)) = 0$.

Example. (i) $F(X,Y) = X + Y$ called $\hat{G}_a$,
(ii) $F(X,Y) = X + Y + XY = (1+X)(1+Y) - 1$ called $\hat{G}_m$,
(iii) $F(X,Y) = X + Y - a_1XY - a_2(X^2Y + XY^2) + \cdots$ called $\hat{E}$.

Definition. Let $\mathcal{F}$ and $\mathcal{G}$ be formal groups over R. A morphism $f\colon \mathcal{F} \to \mathcal{G}$ is a power series $f(X) \in R[[X]]$ with $f(0) = 0$ such that

$$f(F(X,Y)) = G(f(X), f(Y)).$$

We say $\mathcal{F} \cong \mathcal{G}$ if there exist morphisms $f\colon \mathcal{F} \to \mathcal{G}$ and $g\colon \mathcal{G} \to \mathcal{F}$ such that $f(g(T)) = g(f(T)) = T$.

Theorem 7.3. Let $\mathcal{F}$ be a formal group over R with $\operatorname{char}(R) = 0$. Then $\mathcal{F} \cong G_a$ over $R \otimes \mathbb{Q}$. More precisely, there exist a unique power series

$$\log(T) = T + \frac{a_2}{2}T^2 + \frac{a_3}{3}T^3 + \cdots$$

with $a_i \in R$ such that

$$\log(F(X,Y)) = \log(X) + \log(Y) \tag{$*$}$$

and there exist a unique power series

$$\exp(T) = T + \frac{b_2}{2!}T^2 + \frac{b_3}{3!}T^3 + \cdots$$

with $b_i \in R$ such that $\exp(\log(T)) = \log(\exp(T)) = T$.

Proof. We begin by showing the first part. Let $F_1(X,Y) = \frac{d}{dX}F(X,Y)$.

(*Uniqueness.*) Let $p(T) = \frac{d}{dT}\log(T) = 1 + a_2T + a_3T^3 + \cdots$. Differentiate ($*$) to get $p(F(X,Y))F_1(X,Y) = p(X) + 0$, put $X = 0$ so that $p(Y)F_1(0,Y) = 1$ and hence $p(Y) = F_1(0,Y)^{-1}$.

(*Existence.*) Let $p(T)$ be as above, define $\log(T) = T + \frac{a_2}{2}T^2 + \cdots$. Differentiate the associativity law with respect to X to find $F_1(X,F(Y,Z)) = F_1(F(X,Y),Z)F_1(X,Y)$ and put $X = 0$ so $F_1(0,F(Y,Z)) = F_1(Y,Z)F_1(0,Y)$. Therefore,

$$p(F(Y,Z))^{-1} = F_1(Y,Z)p(Y)^{-1}$$

$$\begin{aligned} &\implies && p(Y) = F_1(Y,Z)p(F(Y,Z)) \\ &\implies && \frac{d}{dY}\log Y = \frac{d}{dY}\log F(Y,Z) \\ &\implies && \log F(Y,Z) = \log Y + h(Z) \end{aligned}$$

for some $h(Z) \in R[[Z]]$. By the symmetry between X and Z we see $h(Z) = \log Z$. □

For the second part, we can use the following lemma.

Lemma 7.4. Let $f(T) = aT + \cdots \in R[[T]]$ with $a \in R^\times$ then there exists a unique $g(T) = a^{-1}T + \cdots \in R[[T]]$ such that $f(g(T)) = g(f(T)) = T$.

Proof. We construct polynomials $g_n(T) \in R[T]$ satisfying

$$\begin{aligned} f(g_n(T)) &\equiv T \pmod{T^{n+1}}, \\ g_{n+1}(T) &\equiv g_n(T) \pmod{T^{n+1}}. \end{aligned}$$

Initially we set $g_1(T) = a^{-1}T$. Suppose we have $g_{n-1}(T)$. Then $f(g_{n-1}(T)) \equiv T + bT^n \pmod{T^{n+1}}$ for some $b \in R$. Put $g_n(T) = g_{n-1}(T) + \lambda T^n$ for some $\lambda \in R$ yet to be chosen. Then

$$f(g_n(T)) = f(g_{n-1}(T) + \lambda T^n) \equiv f(g_{n-1}(T)) + \lambda a T^n \equiv T + bT^n + \lambda a T^n \pmod{T^{n+1}}$$

so take $\lambda = -a^{-1}b$ as $a \in R^\times$. Then set

$$g(T) = \lim_{n\to\infty} g_n(T) = a^{-1}T + \cdots \in R[[T]]$$

with $f(g(T)) = T$.

Applying the above $g(T)$, we find

$$h(T) = aT + \cdots \in R[[T]]$$

with $g(h(T)) = T$. But then $f(T) = f(g(h(T))) = h(T)$. □

To prove the second part of Theorem 7.3, it remains to show $b_i \in R$, not just in $R \otimes \mathbb{Q}$. We omit the details but give the following hint: If we differentiate $\log(\exp(T)) = T$ n times and put $T = 0$ then this gives a formula for b_n in terms of $b_1, \ldots, b_{n-1}$ and $a_1, \ldots, a_n$.

Let $\mathcal{F}$ be a formal group. Multiplication by $n \in \mathbb{Z}$ is given by $[n] \in R[[T]]$ where $[0](T) = 0$, $[n+1](T) = F([n]T, T)$ and $[n-1](T) = F([n]T, \iota(T))$.

Remark. $[n]\colon \mathcal{F} \to \mathcal{F}$ is a morphism.

Corollary 7.5. If $n \in R^\times$ is a unit then $[n]\colon \mathcal{F} \to \mathcal{F}$ is an isomorphism.

Proof. By induction, we have $[n](T) = nT + \cdots$ and apply Lemma 7.4. □

Take a ring R, complete with respect to an ideal $I \lhd R$, and for $x, y \in I$ define $x \oplus_{\mathcal{F}} y = F(x,y) \in I$. Then $(I, \oplus_{\mathcal{F}})$ is an abelian group.

Example. $\hat{G}_a(I) = (I, +)$, $\hat{G}_m(I) = (1 + I, \times)$.

Chapter 8

Elliptic Curves over Local Fields

Assume that K is complete with respect to a discrete valuation $\mathrm{ord}_K\colon K^* \to \mathbb{Z}$. Denote the ring of integers by $\mathcal{O}_K = \{x \in K^* : \mathrm{ord}_K(x) \geq 0\} \cup \{0\}$ and its units by $\mathcal{O}_K^* = \{x \in K^* : \mathrm{ord}_K(x) = 0\}$. We pick $\pi \in K$ with $\mathrm{ord}_K(\pi) = 1$ and have the maximal ideal $(\pi) = \pi\mathcal{O}_K = \{x \in K^* : \mathrm{ord}_K(x) \geq 1\} \cup \{0\}$. The residue field is $k = \mathcal{O}_K/\pi\mathcal{O}_K$.

Moreover, assume that $\mathrm{char}(K) = 0$ and $\mathrm{char}(k) = p > 0$, e.g., $K = \mathbb{Q}_p$, $\mathcal{O}_K = \mathbb{Z}_p = \varprojlim_n (\mathbb{Z}/p^n\mathbb{Z})$, $\pi\mathcal{O}_K = p\mathbb{Z}_p$ and $k = \mathbb{F}_p$.

Remark. $\mathrm{ord}_K(x+y) \geq \min\{\mathrm{ord}_K(x), \mathrm{ord}_K(y)\}$ with equality if $\mathrm{ord}_K(x) \neq \mathrm{ord}_K(y)$.

Definition. A Weierstrass equation for E/K is *integral* if $a_1, \ldots, a_6 \in \mathcal{O}_K$ and *minimal* if $\mathrm{ord}_K(\Delta)$ is minimal among all integral equations.

Remark. (i) Putting $x = u^2x'$, $y = u^3y'$ gives $a_i' = u^{-i}a_i$, so we can clear denominators and hence integral equations exist.
(ii) Since $a_1, \ldots, a_6 \in \mathcal{O}_K$, $\Delta \in \mathcal{O}_K$, so $\mathrm{ord}_K(\Delta) \in \mathbb{Z}_{\geq 0}$ and minimal equations exist.

Lemma 8.1. Suppose E/K has Weierstrass equation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. If $\mathcal{O}_E \neq P \in E(K)$, say $P = (x, y)$, then either $x, y \in \mathcal{O}_K$ or $\mathrm{ord}_K(x) = -2r$ and $\mathrm{ord}_K(y) = -3r$ for some $r \in \mathbb{Z}$ with $r \geq 1$.

Proof. Let $s = \mathrm{ord}_K(x)$ and $t = \mathrm{ord}_K(y)$. We consider two cases.

- Case $s \geq 0$. If $t < 0$ then $\mathrm{ord}_K(LHS) = 2t$ and $\mathrm{ord}_K(RHS) \geq 0$, a contradiction. So $t \geq 0$ and $x, y \in \mathcal{O}_K$.
- Case $s < 0$. $\mathrm{ord}_K(LHS) \geq \min\{2t, s+t, t\}$ and $\mathrm{ord}_K(RHS) = 3s$. Looking at all three cases for the minimum, we find $t < s < 0$. Then $\mathrm{ord}_K(LHS) = 2t$ and hence $s = -2r$ and $t = -3r$ for some $r \geq 1$. □

Definition. For $r \geq 1$ let

$$E_r(K) = \{(x, y) \in E(K) : \mathrm{ord}_K(x) \leq -2r, \mathrm{ord}_K(y) \leq -3r\} \cup \{\mathcal{O}_K\}.$$

Proposition 8.2. Let E/K be given with an integral equation and formal group $\hat{E}$ over $\mathcal{O}_K$. For $r \in \mathbb{Z}$ with $r \geq 1$ we have that

(i) $E_r(K) \subset E(K)$ is a subgroup and
(ii) $E_r(K) \cong \hat{E}(\pi^r\mathcal{O}_K)$, $(x, y) \mapsto -x/y$ is an isomorphism.

Proof. Recall that with $t = -x/y$ and $w = -1/y$ we have

$$w = t^3 + a_1tw + a_2t^2 + a_3w^2 + a_4tw^2 + a_6w^3. \tag{$*$}$$

So if $P = (x, y) \in E(K)$ and $s \geq 1$ is an integer then

$$\operatorname{ord}_K(x) = -2s, \operatorname{ord}_K(y) = -3s \quad \Longleftrightarrow \quad \operatorname{ord}_K(t) = s, \operatorname{ord}_K(w) = 3s$$

as $\operatorname{ord}_K(\cdot)$ is multiplicative. Hensel's Lemma 7.1 implies that for each $t \in \pi^r\mathcal{O}_K$ there exists a unique $w \in \pi^{3r}\mathcal{O}_K$ satisfying ($*$). Therefore,

$$E_r(K) \to \pi^r\mathcal{O}_K, (x, y) \mapsto t = -x/y$$

is a bijection. So we can put a group law on it to get $E_r(K) \to \hat{E}(\pi^r\mathcal{O}_K)$. By Proposition 7.2 this is a group homomorphism. □

Proposition 8.3. Let $\mathcal{F}$ be a formal group over $\mathcal{O}_K$. Let $e = \operatorname{ord}_K(p)$. If $r > e/(p-1)$ then $\log\colon \mathcal{F}(\pi^r\mathcal{O}_K) \xrightarrow{\sim} \hat{G}_a(\pi^r\mathcal{O}_K)$ is an isomorphism with inverse $\exp(\cdot)$.

Proof. Let $x \in \pi^r\mathcal{O}_K$. We must show that the power series in Theorem 7.3 converge. Recall that

$$\exp(x) = x + \frac{b_2}{2!}x^2 + \frac{b_3}{3!}x^3 + \cdots$$

with $b_i \in \mathcal{O}_K$. With $e = \operatorname{ord}_K(p)$ and $p = \operatorname{char}(k)$ we have

$$\operatorname{ord}_K(n!) = e\sum_{i=1}^{\infty}\left\lfloor\frac{n}{p_i}\right\rfloor \leq e\sum_{i=1}^{\lfloor\log_p n\rfloor}\frac{n}{p^i} = en\frac{1-p^{-\lfloor\log_p n\rfloor}}{p-1} \leq en\frac{1-1/n}{p-1} = \frac{e(n-1)}{p-1}$$

so if $x \in \pi^r\mathcal{O}_K$ then

$$\operatorname{ord}_K\left(\frac{b_nx^n}{n!}\right) \geq nr - \frac{e(n-1)}{p-1} = r + (n-1)\left(r - \frac{e}{p-1}\right) \geq r,$$

using that $r > e/(p-1)$. Thus $\exp(x) \in \pi^r\mathcal{O}_K$. The case of $\log(\cdot)$ is handled similarly. □

Lemma 8.4. If $\mathcal{F}$ is a formal group over $\mathcal{O}_K$ then, for $r \geq 1$,

$$\mathcal{F}(\pi^r\mathcal{O}_K)/\mathcal{F}(\pi^{r+1}\mathcal{O}_K) \cong (k, +).$$

Proof. $F(X, Y) = X + Y + XY(\cdots)$ so if $x, y \in \pi^r\mathcal{O}_K$ then $F(x, y) \equiv x + y \pmod{\pi^{r+1}}$. Then $\mathcal{F}(\pi^r\mathcal{O}_K) \to k, \pi^r x \mapsto x \pmod{\pi}$ is a group homomorphism with kernel $\mathcal{F}(\pi^{r+1}\mathcal{O}_K)$. □

Proposition 8.5. Suppose $\mathcal{F}$ is a formal group over $\mathcal{O}_K$.

(i) If $p \nmid n$ then $[n]\colon \mathcal{F}(\pi\mathcal{O}_K) \to \mathcal{F}(\pi\mathcal{O}_K)$ is an isomorphism.
(ii) If k is finite then $\mathcal{F}(\pi\mathcal{O}_K)$ contains a subgroup of finite index isomorphic $(\mathcal{O}_K, +)$.

Proof. (i) By our assumption, $n \in \mathcal{O}_K^\times$. Now apply Corollary 7.5.

(ii) We have the following chain of subgroups:

$$(\mathcal{O}_K,+)\cong(\pi^r\mathcal{O}_K,+)\cong\hat{G}_a(\pi^r\mathcal{O}_K)\cong\mathcal{F}(\pi^r\mathcal{O}_K)\subset\cdots\subset\mathcal{F}(\pi^2\mathcal{O}_K)\subset\mathcal{F}(\pi\mathcal{O}_K)$$

where the third isomorphism is present provided $r>e/(p-1)$ and all quotients $\mathcal{F}(\pi^i\mathcal{O}_K)/\mathcal{F}(\pi^{i+1}\mathcal{O}_K)$ are isomorphic to $(k,+)$ by Lemma 8.4. □

Notation. Denote the natural projection by $\tilde{\cdot}$, that is, $\mathcal{O}_K\to\mathcal{O}_K/\pi\mathcal{O}_K=k, x\mapsto\tilde{x}$. The reduction of an integral Weierstrass equation for E/K is

$$\tilde{E}\colon y^2+\tilde{a}_1xy+\tilde{a}_3y=x^3+\tilde{a}_2x^2+\tilde{a}_4x+\tilde{a}_6.$$

Note that $\tilde{E}/k$ is an elliptic curve if and only if $\tilde{\Delta}\neq 0$ if and only if $\mathrm{ord}_K(\Delta)=0$.

Lemma 8.6. If E_1 and E_2 are minimal Weierstrass equations for the same elliptic curve E over K then $\tilde{E}_1\cong\tilde{E}_2$ as curves.

Proof. Say E_1 and E_2 are related by (u,r,s,t) for $u,r,s,t\in K$ with $u\neq 0$. Then $\Delta_1=u^{12}\Delta_2$ so $\mathrm{ord}_K(\Delta_1)=12\,\mathrm{ord}_K(u)+\mathrm{ord}_K(\Delta_2)$. As E_1 and E_2 are minimal, we have $\mathrm{ord}_K(u)=0$s o $u\in\mathcal{O}_K^\times$. By the translation formulae, $r,s,t\in\mathcal{O}_K$. Then $(\tilde{u},\tilde{r},\tilde{s},\tilde{t})$ is a transformation showing $\tilde{E}_1\cong\tilde{E}_2$ over k. □

As a convention, the reduction $\tilde{E}/k$ of E/K is the reduction of a minimal Weierstrass equation.

Definition. E has *good reduction* if $\tilde{E}$ is non-singular, *bad reduction* otherwise.

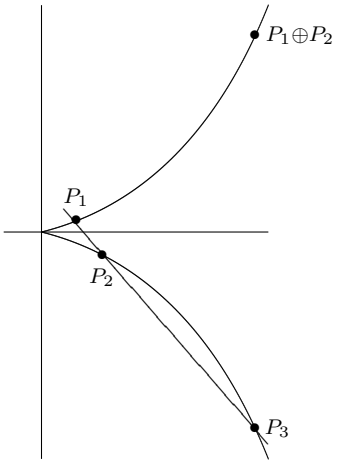
There is a well-defined map $\mathbb{P}^2(K)\to\mathbb{P}^2(k),(x:y:z)\mapsto(\tilde{x}:\tilde{y}:\tilde{z})$ by choosing $(x:y:z)$ with $\min\{\mathrm{ord}_K(x),\mathrm{ord}_K(y),\mathrm{ord}_K(z)\}=0$. This restricts to a map $E(K)\to\tilde{E}(k),P\mapsto\tilde{P}$. We set

$$E_1(K)=\{P\in E(K):\tilde{P}=\mathcal{O}_{\tilde{E}}\},$$

$$\tilde{E}_{ns}=\begin{cases}\tilde{E} & E\text{ has good reduction},\\ \tilde{E}-\{\text{singular point}\} & \text{otherwise.}\end{cases}$$

Fact. The chord-and-tangent process makes $\tilde{E}_{ns}$ a group.

Assume for simplicity that $\mathrm{char}(K)\neq 2$. If $\tilde{E}\colon y^2=f(x)$ is singular then there are two cases. (i) f has a double root, $\tilde{E}_{ns}\cong G_m$, called multiplicative reduction, (ii) f has a triple root, $\tilde{E}_{ns}\cong G_a$, called additive reduction. We give details of the second case:



With $x_i^3 = y_i^2 = y_i^2(ax_i + by_i)$ we see $t_i^3 = at_i + b$ so t_1, t_2, t_3 are roots of $X^3 - aX - b$ and hence $t_1 + t_2 + t_3 = 0$.

Hence the map $\tilde{E}_{ns} \to G_a, (x, y) \to t = x/y$ is a group homomorphism.

Definition.

$$E_0(K) = \{P \in E(K) : \tilde{P} \text{ is smooth on } \tilde{E}\}.$$

Proposition 8.7. $E_0(K) \subset E(K)$ is a subgroup and reduction modulo π defines a surjective group homomorphism $E_0(K) \to \tilde{E}_{ns}(k)$.

Proof. (*Group homomorphism.*) If $P_1, P_2, P_3 \in E(K)$ with $P_1 \oplus P_2 \oplus P_3 = \mathcal{O}_E$. Then they lie on a line ℓ: $a_1X + a_2Y + a_3Z = 0$ for $a_1, a_2, a_3 \in K$ with $\min(\mathrm{ord}_K(a_i)) = 0$. So if $P_1, P_2 \in E_0(K)$ then $\tilde{P}_1, \tilde{P}_2 \in \tilde{E}_{ns}(k)$ and $\tilde{P}_1$, $\tilde{P}_2$, $\tilde{P}_3$ lie on the line $\tilde{\ell}$: $\tilde{a}_1X + \tilde{a}_2Y + \tilde{a}_3Z = 0$. The group law on $\tilde{E}_{ns}(k)$ implies $\tilde{P}_3 \in \tilde{E}_{ns}(k)$ so $P_3 \in E_0(K)$ and $\tilde{P}_1 + \tilde{P}_2 + \tilde{P}_3 = \mathcal{O}_{\tilde{E}}$. One also needs to check multiplicities.

(*Surjective.*) Let $f(x, y) = y^2 + a_1xy + a_3y - (x^3 + a_2x^2 + a_4x + a_6)$ and take $\mathcal{O}_{\tilde{E}} \neq \tilde{P} \in \tilde{E}_{ns}(k)$, say $\tilde{P} = (\tilde{x}_0, \tilde{y}_0)$ for some $x_0, y_0 \in \mathcal{O}_K$. Then $f(x_0, y_0) \equiv 0 \pmod{\pi}$. If $\tilde{P}$ is smooth then either $\partial f/\partial x(x_0, y_0) \not\equiv 0 \pmod{\pi}$ or $\partial f/\partial y(x_0, y_0) \not\equiv 0$. In the first case, put $g(X) = f(X, y_0) \in \mathcal{O}_K[X]$. Then $g(x_0) \equiv 0 \pmod{\pi}$, $g'(x_0) \in \mathcal{O}_K^\times$ and by Hensel's Lemma 7.1 there exists a $b \in \mathcal{O}_K$ such that $g(b) = 0$ and $b \equiv x_0 \pmod{\pi}$. Then $P = (x_0, y_0) \in E(K)$ with $\tilde{P} = (\tilde{x}_0, \tilde{y}_0)$. The second case is dealt with separable. □

Recall the following chain of subgroups:

$$(\mathcal{O}_K, +) \cong E_r(K) \subset \cdots \subset E_2(K) \subset E_1(K) \subset E_0(K) \subset E(K)$$

where we assume $r > e/(p-1)$ and we know that $E_i(K)/E_{i+1}(K) \cong (k, +)$ for $i \geq 1$ and $E_0(K)/E_1(K) \cong \tilde{E}_{ns}(k)$. So far, we do not know much about the quotient $E(K)/E_0(K)$.

Definition. The *Tamagawa number* is $c_K(E) = |E(K)/E_0(K)|$.

Remark. Good reduction implies that $c_K(E) = 1$, but the converse is not true.

Fact. Either $c_K(E) = \mathrm{ord}_K(\Delta)$ or $c_K(E) \leq 4$.

Lemma 8.8. If $|k| < \infty$ then $\mathbb{P}^n(K)$ is compact with respect to the π-adic topology.

Proof. $\mathcal{O}_K = \varprojlim_n \mathcal{O}_K/\pi^n\mathcal{O}_K$ is profinite hence compact. Then $\mathbb{P}^n(K)$ is a union of sets

$$U_i = \{(x_0 : \cdots : x_n) \in \mathbb{P}^n(K) : x_0, \ldots, x_n \in \mathcal{O}_K, x_i = 1\}.$$

As $\mathcal{O}_K$ is compact, we have that $U_i \cong \mathcal{O}_K^n$ is compact, so $\mathbb{P}^n(K)$ is compact. □

Lemma 8.9. If $|k| < \infty$ then $c_K(E) < \infty$.

Proof. The formulae for the group law imply that $\oplus$: $E \times E \to E$ and $[-1]$: $E \to E$ are continuous, so $(E, \oplus)$ is a topological group. $E(K) \subset \mathbb{P}^2(K)$ is a closed subgroup. Hence, by Lemma 8.8, $E(K)$ is compact. Let $(\tilde{x}_0, \tilde{y}_0)$ be the singular point on $\tilde{E}$, for otherwise we are done, with $x_0, y_0 \in \mathcal{O}_K$. The set

$$E(K) \setminus E_0(K) = \{(x, y) \in E(K) : \mathrm{ord}_K(x - x_0) \geq 1, \mathrm{ord}_K(y - y_0) \geq 1\}$$

is a closed subset of $E(K)$, so $E_0(K) \subset E(K)$ is an open subgroup. The cosets of $E_0(K)$ give an open cover of $E(K)$ and hence by compactness $c_K(E) < \infty$. □

Theorem 8.10. If $|k| < \infty$ then $E(K)$ contains a subgroup $E_r(K)$ of finite index with $E_r(K) \cong (\mathcal{O}_K, +)$. Moreover, $E(K)_{tors}$ is finite.

Proof. See above. Note that $(\mathcal{O}_K, +)$ is torsion-free so $E(K)_{tors} \hookrightarrow E(K)/E_r(K)$. □

Now assume that $[K : \mathbb{Q}_p] < \infty$, L/K is a finite extension and $[L : K] = ef$ where

$$\begin{array}{ccc} K^* & \xrightarrow{\text{ord}_K} & \mathbb{Z} \\ \downarrow & & \downarrow \times e \\ L^* & \xrightarrow{\text{ord}_L} & \mathbb{Z} \end{array}$$

and $f = [\ell : k]$, ℓ and k being the residue fields of L and K, respectively.

Definition. L/K is *unramified* if $e = 1$.

Fact. For each integer $n \geq 1$,

(i) k has a unique extension of degree n,
(ii) K has a unique unramified extension of degree n.

Definition. K^{nr} is the maximal unramified extension of K. It has residue field $\bar{k}$, the algebraic closure of k.

Proposition 8.11. If E/K has good reduction at $p \nmid n$ then

(i) $E(K^{nr})[n] = E(\bar{K})[n]$,
(ii) $E(K^{nr}) \xrightarrow{\times n} E(K^{nr})$ is surjective.

Proof. We have a commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E_1(K^{nr}) & \longrightarrow & E(K^{nr}) & \longrightarrow & \tilde{E}(\bar{k}) & \longrightarrow & 0 \\ & & \cong \downarrow \times n & & \downarrow \times n & & \downarrow \times n & & \\ 0 & \longrightarrow & E_1(K^{nr}) & \longrightarrow & E(K^{nr}) & \longrightarrow & \tilde{E}(\bar{k}) & \longrightarrow & 0 \end{array}$$

using Proposition 8.5 and Theorem 2.5. By the Snake Lemma,

$$E(K^{nr})[n] \cong \tilde{E}(\bar{k})[n], \qquad E(K^{nr})/nE(K^{nr}) = 0$$

showing (ii). By Theorem 6.5, $\tilde{E}(\bar{k})[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$ and also $E(K^{nr})[n] \subset E(\bar{K})[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$ so $E(K^{nr})[n] = E(\bar{K})[n]$. □

Corollary 8.12. Suppose E/K has good reduction at $p \nmid n$. If $P \in E(K)$ then $K([n]^{-1}P)$ is an unramified extension of K.

Notation. $[n]^{-1}P = \{Q \in E(\bar{K}) : nQ = P\}$. If $P_1, \ldots, P_r \in E(\bar{K})$ then with $P_i = (x_i, y_i)$ we set $K(P_1, \ldots, P_r) = K(x_1, y_1, \ldots, x_r, y_r)$.

Proof. By the second part of Proposition 8.11, $P = nQ$ for some $Q \in E(K^{nr})$. Then $[n]^{-1}P = \{Q + T : T \in E(\bar{K})[n]\}$. The first part of Proposition 8.11 implies that $E(\bar{K})[n] = E(K^{nr})[n]$ so $[n]^{-1}P \subset E(K^{nr})$. □

Chapter 9

Elliptic Curves over Number Fields: The Torsion Subgroup

Assume that K is a number field, that is, $[K:\mathbb{Q}] < \infty$.

Notation. For P a prime of K let K_P be the P-adic completion of K and $k_P = \mathcal{O}_K/P$.

Definition. E/K has *good (resp. bad) reduction* at P if E/K_P has good (resp. bad) reduction.

Lemma 9.1. E has only finitely many bad primes.

Proof. Take a Weierstrass equation with $a_1, \ldots, a_6 \in \mathcal{O}_K$. As E is non-singular we have $0 \neq \Delta \in \mathcal{O}_K$ so $(\Delta) = P_1^{\alpha_1} \cdots P_r^{\alpha_r}$ for distinct primes P_i in K. Now let $S = \{P_1, \ldots, P_r\}$. If $P \notin S$ then $\mathrm{ord}_P(\Delta) = 0$ so E has good reduction at P. So all bad primes lie in S. □

Remark. If K has class number 1, e.g., $K = \mathbb{Q}$, then we can find a Weierstrass equation for E that is minimal at all primes P of K.

Lemma 9.2. $E(K)_{tors}$ is finite.

Proof. For any prime P, if $K \subset K_P$ then $E(K) \subset E(K_P)$ and $E(K)_{tors} \subset E(K_P)_{tors}$. Now apply Theorem 8.10. □

Lemma 9.3. Suppose that E has good reduction at P where $P \nmid (n)$. Then reduction modulo P defines an injection

$$E(K)[n] \hookrightarrow \tilde{E}(k_P)[n].$$

Proof. $E_1(K_P) = \ker\big(E(K_P) \to \tilde{E}(k_P)\big)$ has no n-torsion by Proposition 8.5. □

Example. Consider $E\colon y^2 + y = x^3 - x$, $\Delta = -11$, which has good reduction at $p \neq 11$.

p	2	3	5	7	11	13
$\lvert\tilde{E}(\mathbb{F}_p)\rvert$	5	5	5	10		10

So $|E(\mathbb{Q})_{tors}| \mid 5 \cdot 2^a$ for some $a \geq 0$ and $|E(\mathbb{Q})_{tors}| \mid 5 \cdot 3^b$ for some $b \geq 0$.

Example. Consider $E\colon y^2 + y = x^3 + x^2$, $\Delta = -43$, which has good reduction at $p \neq 43$.

p	2	3	5	7	11	13
$\lvert\tilde{E}(\mathbb{F}_p)\rvert$	5	6	10	8	9	19

So $|E(\mathbb{Q})_{tors}| \mid 5 \cdot 2^a$ for some $a \geq 0$ and $|E(\mathbb{Q})_{tors}| \mid 9 \cdot 11^b$ for some $b \geq 0$. Thus we have $E(\mathbb{Q})_{tors} = \{\mathcal{O}_E\}$, so $T = (0,0) \in E(\mathbb{Q})$ has infinite order and $\operatorname{rank} E(\mathbb{Q}) \geq 1$.

Lemma 9.4. Suppose $E/\mathbb{Q}$ has Weierstrass equation with $a_1, \ldots, a_6 \in \mathbb{Z}$. Suppose that $\mathcal{O}_E \neq T = (x,y) \in E(\mathbb{Q})_{tors}$. Then $4x, 8y \in \mathbb{Z}$ and, moreover, if $2 \mid a_1$ or $2T \neq \mathcal{O}_E$ then $x, y \in \mathbb{Z}$.

Proof. The Weierstrass equation determines a formal group $\hat{E}$ over $\mathbb{Z}$. For a prime p and an integer $r \geq 1$ we recall that $E_r(\mathbb{Q}_p) \cong \hat{E}(p^r\mathbb{Z}_p)$ where

$$E(\mathbb{Q}_p) \setminus E_1(\mathbb{Q}_p) = \{(x,y) \in E(\mathbb{Q}_p) : \operatorname{ord}_p(x) \geq 0, \operatorname{ord}_p(y) \geq 0\},$$
$$E_r(\mathbb{Q}_p) \setminus E_{r+1}(\mathbb{Q}_p) = \{(x,y) \in E_r(\mathbb{Q}_p) : \operatorname{ord}_p(x) \geq -2r, \operatorname{ord}_p(y) \geq -3r\}.$$

By Proposition 8.3, $\hat{E}(p^r\mathbb{Z}_p) \cong (\mathbb{Z}_p, +)$ if $r > 1/(p-1)$, so $(x,y) \in E(\mathbb{Q})_{tors}$ and hence $\operatorname{ord}_p(x), \operatorname{ord}_p(y) \geq 0$, except possibly if $p = 2$ when we could have $\operatorname{ord}_2(x) = -2$, $\operatorname{ord}_2(y) = -3$. In this case $T \in E_1(\mathbb{Q}_2) \setminus E_2(\mathbb{Q}_2)$ but

$$E_1(\mathbb{Q}_2)/E_2(\mathbb{Q}_2) \cong (\mathbb{F}_2, +)$$

and $E_2(\mathbb{Q}_2) \cong (\mathbb{Z}, +)$ so is torsion-free. So $2T = \mathcal{O}_E$. Also $(x,y) = T = \ominus T = (x, -y - a_1x - a_3)$ so $2y + a_1x + a_3 = 0$ and from $\operatorname{ord}_2(2y) = -2$, $\operatorname{ord}_2(a_3) \geq 2$ we have that $\operatorname{ord}_2(a_1x) = -2$ so a_1 is odd. The result follows. □

Example. Consider $E\colon y^2 + xy = x^3 + 4x + 1$ and note $(-1/4, 1/8) \in E(\mathbb{Q})[2]$.

Corollary 9.5 (Lutz–Nagell)**.** Suppose $E/\mathbb{Q}\colon y^2 = x^3 + ax + b$ with $a, b \in \mathbb{Z}$. If $\mathcal{O}_E \neq T = (x,y) \in E(\mathbb{Q})_{tors}$ then $x, y \in \mathbb{Z}$ and either $y = 0$ or $y^2 \mid 4a^3 + 27b^2$.

Proof. By Lemma 9.4, $x, y \in \mathbb{Z}$. If $2T = \mathcal{O}_E$ then $y = 0$. If note, $2T = (x_2, y_2)$ and by Lemma 9.4, $x_2, y_2 \in \mathbb{Z}$. Let $f(X) = X^3 + aX + b$. Then $x_2 = (f'(x)/2y)^2 - 2x$ hence $y \mid f'(x)$ and now recall that $y^2 = f(x)$. As E is non-singular, $f(X)$ and $f'(X)$ are coprime so $f(X)$ and $f'(X)^2$ are coprime. Using Euclid's algorithm, we find $g, h \in \mathbb{Q}[X]$ such that $g(X)f(X) + h(X)f'(X)^2 = 1$. A calculation shows that

$$(3x^2 + 4a)f'(X)^2 - 27(X^3 + aX - b)f(X) = 4a^3 + 27b^2.$$

Finally, since $y \mid f'(X)$ and $y^2 = f(X)$ we have $y^2 \mid 4a^3 + 27b^2$. □

Example. Consider $E_D\colon y^2 = x^3 - D^2x = f(x)$ where $D \in \mathbb{Z}$ is square-free and $\Delta = 2^6D^6$. We know $E_D(\mathbb{Q})_{tors} \supset \{\mathcal{O}_E, (0,0), (D,0), (-D,0)\}$. If $p \nmid 2D$ then

$$|\tilde{E}_D(\mathbb{F}_p)| = 1 + \sum_{x \in \mathbb{F}_p} \left(\left(\frac{f(x)}{p} \right) + 1 \right).$$

If $p \equiv 3 \pmod 4$,

$$\left(\frac{f(-x)}{p} \right) = \left(\frac{-f(x)}{p} \right) = \left(\frac{-1}{p} \right) \left(\frac{f(x)}{p} \right) = - \left(\frac{f(x)}{p} \right)$$

so $|\tilde{E}_D(\mathbb{F}_p)| = p+1$. Let $m = |\tilde{E}_D(\mathbb{Q})_{tors}|$ then $4 \mid m \mid p+1$, for all sufficiently large primes p with $p \equiv 3 \pmod 4$. Thus $m = 4$, otherwise we have a contradiction to Dirichlet's theorem on primes in arithmetic progression. So $|E_D(\mathbb{Q})_{tors}| =$ and $E_D(\mathbb{Q})_{tors} \cong (\mathbb{Z}/2\mathbb{Z})^2$. So $\operatorname{rank} E_D(\mathbb{Q}) \geq 1$ if and only if there exist $x, y \in \mathbb{Q}$ with $y \neq 0$ and $y^2 = x^3 - D^2x$, that is, if and only if D is a congruent number.

Remark. Mazur has shown that if $E/\mathbb{Q}$ is an elliptic curve then

$$E(\mathbb{Q})_{tors} = \begin{cases} \mathbb{Z}/n\mathbb{Z} & 1 \leq n \leq 12, n \neq 11 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z} & 1 \leq n \leq 4 \end{cases}$$

and all these cases occur.

Definition. Suppose K is a number field, S a finite set of primes in K and $n \geq 2$ an integer. Then we set

$$K(S,n) = \{x \in K^*/(K^*)^n : \forall P \notin S \quad \operatorname{ord}_P(x) \equiv 0 \pmod n\}.$$

Example. $\mathbb{Q}(\{3,17\},2) = \langle -1,3,17\rangle \subset \mathbb{Q}^*/(\mathbb{Q}^*)^2$ where $\langle -1,3,17\rangle \cong (\mathbb{Z}/2\mathbb{Z})^3$.

Proposition 9.6. $K(S,n)$ is finite.

Proof. The proof uses the finiteness of the class group Cl_K and Dirichlet's unit theorem stating that $\mathcal{O}_K^\times$ is finitely generated.

Let I_K be the group of fractional ideals.

$$0 \to K^* \xrightarrow{i} I_K \to \mathrm{Cl}_K \to 0$$

where i is the map $x \mapsto (x)$. Let $P_K = i(K^*)$ be the principal fractional ideals. Apply the Snake Lemma to the two diagrams

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathcal{O}_K^\times & \longrightarrow & K^* & \longrightarrow & P_K & \longrightarrow & 0 \\ & & \downarrow n & & \downarrow n & & \downarrow n & & \\ 0 & \longrightarrow & \mathcal{O}_K^\times & \longrightarrow & K^* & \longrightarrow & P_K & \longrightarrow & 0 \end{array}$$

and

$$\begin{array}{ccccccccc} 0 & \longrightarrow & P_K & \longrightarrow & I_K & \longrightarrow & \mathrm{Cl}_K & \longrightarrow & 0 \\ & & \downarrow n & & \downarrow n & & \downarrow n & & \\ 0 & \longrightarrow & P_K & \longrightarrow & I_K & \longrightarrow & \mathrm{Cl}_K & \longrightarrow & 0 \end{array}$$

to obtain

$$0 \to \mathcal{O}_K^\times/(\mathcal{O}_K^\times)^n \to K^*/(K^*)^n \to P_K/P_K^n \to 0 \tag{1}$$

and

$$0 \to \mathrm{Cl}_K[n] \to P_K/P_K^n \to I_K/I_K^n \to \mathrm{Cl}_K\,/\,\mathrm{Cl}_K^n \to 0. \tag{2}$$

By definition of $K(S,n)$, the image of $K(S,n)$ in I_K/I_K^n is finite. Now (2) and the finiteness of the class group imply that the image of $K(S,n)$ in P_K/P_K^n is finite. Finally, (1) and the fact that $\mathcal{O}_K^\times$ is finitely generated show that $K(S,n)$ is finite. □

Chapter 10

Kummer Theory

Assume that K is any field with $\mathrm{char}(K) \nmid n$ and $\mu_n \subset K$.

Lemma 10.1. Let $\Delta \subset K^*/(K^*)^n$ be a finite subgroup and $L = K(\sqrt[n]{\Delta})$. Then L/K is Galois and $\mathrm{Gal}(L/K) \cong \mathrm{Hom}(\Delta, \mu_n)$.

Proof. We leave the proof that L/K is Galois as an exercise. Define the Kummer pairing by

$$\langle \cdot, \cdot \rangle \colon \mathrm{Gal}(L/K) \times \Delta \to \mu_n, (\sigma, x) \mapsto \left(\frac{\sigma \sqrt[n]{x}}{\sqrt[n]{x}} \right).$$

This is well-defined: If $\alpha, \beta \in L$ with $\alpha^n = \beta^n = x$ then for any $\sigma \in \mathrm{Gal}(L/K)$ we have $(\alpha/\beta)^n = 1$ s $\alpha/\beta \in \mu_n \subset K$ and hence $\sigma(\alpha/\beta) = \alpha/\beta$, that is, $\sigma(\alpha)/\alpha = \sigma(\beta)/\beta$, as required. It is also bilinear as

$$\langle \sigma\tau, x \rangle = \frac{\sigma(\tau \sqrt[n]{x})}{\tau \sqrt[n]{x}} = \langle \sigma, x \rangle \langle \tau, x \rangle,$$
$$\langle \sigma, xy \rangle = \frac{\sigma(\sqrt[n]{x}\sqrt[n]{y})}{\sqrt[n]{x}\sqrt[n]{y}} = \langle \sigma, x \rangle \langle \sigma, x \rangle$$

and non-degenerate: Let $\sigma \in \mathrm{Gal}(L/K)$ and suppose that $\langle \sigma, x \rangle = 1$ for all $x \in \Delta$, so $\sigma(\sqrt[n]{x}) = \sqrt[n]{x}$ for all $x \in \Delta$, that is, σ fixes L pointwise and hence $\sigma = \iota$. Now let $x \in \Delta$ and suppose that $\langle \sigma, x \rangle = 1$ for all $\sigma \in \mathrm{Gal}(L/K)$. Then $\sigma(\sqrt[n]{x}) = \sqrt[n]{x}$ for all $\sigma \in \mathrm{Gal}(L/K)$ and hence $\sqrt[n]{x} \in K$ so $x \in (K^*)^n$, i.e, $x(K^*)^n = 1$ in Δ.

The Kummer pairing introduces group homomorphisms

$$\mathrm{Gal}(L/K) \hookrightarrow \mathrm{Hom}(\Delta, \mu_n) \tag{1}$$

and

$$\Delta \hookrightarrow \mathrm{Hom}(\mathrm{Gal}(L/K), \mu_n). \tag{2}$$

Considering the first of these, we see that $\mathrm{Gal}(L/K)$ is abelian of exponent dividing n and $|\mathrm{Hom}(\mathrm{Gal}(L/K), \mu_n)| = |\mathrm{Gal}(L/K)|$, hence

$$|\mathrm{Gal}(L/K)| \leq |\Delta| \leq |\mathrm{Gal}(L/K)|$$

using the first and second homomorphism to establish the two inequalities. Thus $|\mathrm{Gal}(L/K)| = |\Delta|$ and so (1) and (2) are isomorphism. □

Proposition 10.2. There is a bijection between the finite subgroups $\Delta \subset K^*/(K^*)^n$ and finite abelian extensions L/K of exponent dividing n, given by $\Delta \mapsto K(\sqrt[n]{\Delta})$.

Proof. (*Injective.*) Suppose $K(\sqrt[n]{\Delta_1}) = K(\sqrt[n]{\Delta_2})$. Replacing Δ_2 by $\Delta_1\Delta_2$ we may assume that $\Delta_1 \subset \Delta_2$. Then, by Lemma 10.1, $|\Delta_1| = |\Delta_2|$ and hence $\Delta_1 = \Delta_2$.

(*Surjective.*) Take L/K Galosi with $\mathrm{Gal}(L/K) = G$ abelian of exponent dividing n. Let $\Delta = (K^* \cap (L^*)^n)/(K^*)^n$. Clearly $K(\sqrt[n]{\Delta}) \subset L$. But $[K(\sqrt[n]{\Delta}) : K] = |\Delta|$ by Lemma 10.1 and $[L : K] = |G|$ so it suffices to show that $|\Delta| = |G|$. Recall that the Kummer pairing induces an injection $\Delta \hookrightarrow \mathrm{Hom}(G, \mu_n)$. We claim that this map is also surjective.

Let $\chi \in \mathrm{Hom}(G, \mu_n)$. Distinct automorphisms are linearly independent so we can set

$$y = \sum_{\tau \in G} \chi(\tau)^{-1}\tau(a) \neq 0$$

for some $a \neq 0$ in L. Let $\sigma \in G$, then

$$\begin{aligned}
\sigma(y) &= \sum_{\tau \in G} \chi(\tau)^{-1}\sigma\tau(a) \\
&= \sum_{\tau \in G} \chi(\sigma^{-1}\tau)^{-1}\tau(a) \\
&= \sum_{\tau \in G} \chi(\sigma^{-1})^{-1}\chi(\tau)^{-1}\tau(a) \\
&= \chi(\sigma)y \qquad (*)
\end{aligned}$$

and hence $\sigma(y^n) = y^n$ for all $\sigma \in G$. Now let $x = y^n$ so that $x \in K^* \cap (L^*)^n$, so $x(K^*)^n \in \Delta$ and $\Delta \hookrightarrow \mathrm{Hom}(G, \mu_n), x(K^*)^n \mapsto (\sigma \mapsto \sigma(y)/y) = \chi$, by $(*)$.

So $|\Delta| = |\mathrm{Hom}(G, \mu_n)|$ by the claim, and $|\mathrm{Hom}(G, \mu_n)| = |G|$ since G is abelian of exponent dividing n. □

Proposition 10.3. Suppose K is a number field with $\mu_n \subset K$ and let S be a finite set of primes in K. Then there exists only finitely many extensions L/K such that

(i) L/K is ablean of exponent dividing n,
(ii) L/K is unramified at P for all $P \notin S$.

Proof. Suppose L/K is as in (i) and (ii). By Proposition 10.2, $L = K(\sqrt[n]{\Delta})$ since $\Delta \subset K^*/(K^*)^n$. Let P be a prime of K, $P\mathcal{O}_L = P_1^{e_1} \cdots P_r^{e_r}$ for distinct primes P_i in L. If $x(K^*)^n \in \Delta$ then

$$n \operatorname{ord}_{P_i}(\sqrt[n]{x}) = \operatorname{ord}_{P_i}(x) = e_i \operatorname{ord}_P(x).$$

If $P \notin S$ then $e_1 = \cdots = e_r = 1$ so $\operatorname{ord}_P(x) \equiv 0 \pmod{n}$. Thus

$$\Delta \subset K(S, n) = \{x \in K^*/(K^*)^n : \forall P \notin S \quad \operatorname{ord}_P(x) \equiv 0 \pmod{n}\}$$

and this is finite by Proposition 9.6. So $\Delta \subset K(S, n)$ is finite and there exists only finitely many choices for Δ. □

Chapter 11

Elliptic Curves over Number Fields: The Mordell–Weil Theorem

Theorem 11.1 (Weak Mordell–Weil)**.** Suppose K is a number field, E/K an elliptic curve and $n \geq 2$ an integer. Then

$$|E(K)/nE(K)| < \infty.$$

Lemma 11.2. Assume $E[n] \subset E(K)$, $S = \{\text{bad primes for } E\} \cup \{p \mid n\}$ and $L = K([n]^{-1}P)$ for some $P \in E(K)$. Then

(i) L/K is Galois with $\mathrm{Gal}(L/K)$ abelian of exponent dividing n,
(ii) L/K is unramified at all $p \notin S$.

Proof. Let $Q \in [n]^{-1}P$. Then $L = K(Q)$ since $E[n] \subset E(K)$.

(i) Take $M/L/K$ such that M/K is Galois. Let $\sigma \in \mathrm{Gal}(M/K)$. Then

$$\begin{aligned} & n(\sigma(Q) - Q) = P - P = 0 \\ \implies \quad & \sigma(Q) - Q \in E[n] \subset E(K) \\ \implies \quad & \sigma(Q) \in E(L) \\ \implies \quad & \sigma(L) = L \end{aligned}$$

so L/K is Galois. Now consider the map

$$\phi\colon \mathrm{Gal}(L/K) \to E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2, \sigma \mapsto \sigma(Q) - Q.$$

We claim that ϕ is an embedding. First note that

$$\phi(\sigma\tau) = (\sigma\tau(Q) - \sigma(Q)) + (\sigma(Q) - Q)$$

so ϕ is a group homomorphism. Moreover, if $\sigma(Q) = Q$ then σ fixes L pointwise so $\sigma = \iota$, which shows that ϕ is injective.

(ii) See Corollary 8.12.

□

Lemma 11.3. Suppose that L/K is a finite Galois extension. Then $|E(L)/nE(L)| < \infty$ implies that $|E(K)/nE(K)| < \infty$.

Proof. Postponed, see Page 52. □

Proof (Theorem 11.1). By Lemma 11.3, we may assume that $\mu_n \subset K$ and $E[n] \subset E(K)$. Let L be the composite inside $\bar{K}$ of all fields $K([n]^{-1}P)$ for $P \in E(K)$. By Proposition 10.3 and Lemma 11.2 there are only finitely many such fields. Then we still have $[L : K] < \infty$. There is a "Kummer pairing",

$$\mathrm{Gal}(L/K) \times E(K)/nE(K) \to E[n], (\sigma, P) \mapsto \sigma(Q) - Q$$

where $nQ = P$. We can check that this map is well-defined and bilinear as in the proof of Lemma 10.1. To show that it is injective, let $P \in E(K)$ with $P = nQ$ and Q a point over L then $\sigma(Q) - Q = 0$ for all $\sigma \in \mathrm{Gal}(L/K)$ and hence $Q \in E(K)$ so $P \in nE(K)$. Finally, as $\mathrm{Gal}(L/K)$ and $E[n]$ are finite we conclude that $E(K)/nE(K)$ is finite. □

Remark. If K is $\mathbb{R}$, $\mathbb{C}$ or $\mathbb{Q}_p$ then $|E(K)/nE(K)| < \infty$, yet $E(K)$ is not finitely generated. In fact, it is uncountable.

We will now prove the Mordell–Weil theorem assuming the following statement, which we will establish in the next chapter: If K is a number field then there exists a quadratic form $\hat{h}\colon E(K) \to \mathbb{R}_{\geq 0}$ such that the set $\{P \in E(K) : \hat{h}(P) \leq B\}$ is finite for all $B \geq 0$.

Theorem 11.4 (Mordell–Weil)**.** Suppose that K is a number field and E/K an elliptic curve. Then $E(K)$ is a finitely generated group.

Proof. Weak Mordell–Weil gives $|E(K)/nE(K)| < \infty$. Choose coset representatives $P_1, \ldots, P_r$ and let $\Sigma = \{P \in E(K) : \hat{h}(P) \leq \max_{1 \leq i \leq r} \hat{h}(P_i)\}$.

We claim that Σ generates $E(K)$. Take $P \in E(K) \setminus \langle \Sigma \rangle$ of minimal height, which exists by our earlier assumption. Then $P = P_i + nQ$ for some $1 \leq i \leq r$ and some $Q \in E(K)$. Minimality of $\hat{h}(P)$ implies that $\hat{h}(P) \leq \hat{h}(Q)$. As we assume $n \geq 2$,

$$\begin{aligned} 4\hat{h}(P) \leq 4\hat{h}(Q) \leq n^2\hat{h}(Q) &= \hat{h}(nQ) \\ &= \hat{h}(P - P_i) \\ &\leq \hat{h}(P - P_i) + \hat{h}(P + P_i) = 2\hat{h}(P) + 2\hat{h}(P_i) \end{aligned}$$

so $\hat{h}(P) \leq \hat{h}(P_i)$ and thus $P \in \Sigma$, a contradiction.

Again, by our previously mentioned assumption, Σ is finite and hence $E(K)$ is finitely generated. □

Chapter 12

Heights

For simplicity we assume that $K = \mathbb{Q}$. For $P \in \mathbb{P}^n(\mathbb{Q})$ write $P = (a_0 : \cdots : a_n)$ with $a_0, \ldots, a_n \in \mathbb{Z}$ and $\gcd(a_0, \ldots, a_n) = 1$.

Definition.

$$H(P) = \max_{0 \le i \le n} |a_i|.$$

Remark. For any $B > 0$ the set $\{P \in \mathbb{P}^n : H(P) \le B\}$ is finite.

Definition. A morphism of degree d defined over $\mathbb{Q}$ is a map $F\colon \mathbb{P}^n \to \mathbb{P}^m$, $\mathbb{P} \mapsto (f_0(P) : \cdots : f_m(P))$ where $f_0, \ldots, f_m \in \mathbb{Q}[X_0, \ldots, X_n]$ are homogeneous of degree d and such that the only common zero of $f_0, \ldots, f_n$ over $\bar{Q}$ is $x_0 = \cdots = x_n = 0$.

Proposition 12.1. There exist constants $c_1, c_2 > 0$ depending only on F such that

$$\forall P \in \mathbb{P}(\mathbb{Q}) \quad c_1 H(P)^d \le H(F(P)) \le c_2 H(P)^d.$$

Proof. Without loss of generality $f_0, \ldots, f_m \in \mathbb{Z}[X_0, \ldots, X_n]$.

(*Upper bound.*) Write $P = (a_0 : \cdots : a_n)$ with $a_i \in \mathbb{Z}$ coprime. Then

$$H(F(P)) \le \max_{0 \le j \le m} |f_j(a_0, \ldots, a_n)| \le c_2 \max_{0 \le i \le n} |a_i|^d = c_2 H(P)$$

where $c_2 = \max_{0 \le j \le m}(\text{sum of absolute values of coefficients of } f_j)$.

(*Lower bound.*) We use the *Nullstellensatz*:

Let $K = \bar{K}$ and $I \subset K[X_0, \ldots, X_n]$ an ideal, and set $V(I) = \{(a_0, \ldots, a_n) \in K^{n+1} : \forall f \in I \quad f(a_0, \ldots, a_n) = 0\}$. If $f \in K[X_0, \ldots, X_n]$ vanishes on $V(I)$ then $f^r \in I$ for some $r \in \mathbb{N}$.

We apply this with $I = (f_0, \ldots, f_m)$. F is a morphism so $V(I) = \{(0, \ldots, 0)\}$. Then there exist $g_{ij} \in \bar{\mathbb{Q}}[X_0, \ldots, X_n]$ and $r \ge 1$ such that

$$\forall\, 0 \le i \le n \quad \sum_{j=0}^{m} g_{ij} f_j = X_i^r.$$

Given r, we can solve for the coefficients by linear algebra, so without loss of generality we have $g_{ij} \in \mathbb{Q}[X_0, \ldots, X_n]$. Also, without loss of generality, g_{ij} is homogeneous of degree $r - d$. Clearing denominators, we have $\sum_{j=0}^{m} g_{ij} f_j = K X_i^r$ for some $g_{ij} \in \mathbb{Z}[X_0, \ldots, X_n]$ and $K \in \mathbb{N}$. Writing $P = (a_0 : \cdots : a_n)$ with $a_i \in \mathbb{Z}$ coprime, we

have that $\sum_{j=0}^{m} g_{ij}(a_0,\dots,a_n)f_j(a_0,\dots,a_n) = Ka_i^r$ for all $0 \le i \le n$. This gives that $\gcd(f_0(a_0,\dots,a_n),\dots,f_m(a_0,\dots,a_n)) \mid K$. Therefore,

$$H(F(P)) \ge \frac{1}{K} \max_{0\le j\le m} |f_j(a_0,\dots,a_n)|.$$

So

$$|Ka_i^r| \le KH(F(P))\delta_i \Big(\max_{0\le j\le m} |a_j|\Big)^{r-d}$$

where $\delta_i = \sum_{j=0}^{m}$(sum of absolute values of coefficients of g_{ij}) so

$$KH(P)^r \le KH(F(P))\Big(\max_{0\le i\le n} \delta_i\Big) H(P)^{r-d}$$

and hence $c_1 H(P)^d \le H(F(P))$ where $c_1 = 1/\max_{0\le i\le n} \delta_i$. □

Definition. For $x \in \mathbb{Q}$ set $H(x) = H((x:1))$, that is,

$$H\Big(\frac{a}{b}\Big) = \max\{|a|,|b|\}$$

where $(a,b) = 1$.

Corollary 12.2. Let $f, g \in \mathbb{Q}[X]$ be coprime with $\max\{\deg(f),\deg(g)\} = d$. Then there exist $c_1, c_2 > 0$ such that

$$c_1 H(x)^d \le H\left(\frac{f(x)}{g(x)}\right) \le c_2 H(x)^d$$

for all $x \in \mathbb{Q}$ with $g(x) \ne 0$.

Proof. This is the case $m = n = 1$ in Proposition 12.1. □

Definition. The *height* of an elliptic curve E over $\mathbb{Q}$ is

$$H\colon E(\mathbb{Q}) \to \mathbb{R}_{\ge 1}, P \mapsto \begin{cases} H(x) & P = (x,y), \\ 1 & P = \mathcal{O}_E. \end{cases}$$

The *logarithmic height* is $h\colon E(Q) \to \mathbb{R}_{\ge 0}, P \mapsto \log H(P)$.

Lemma 12.3. Suppose that E and E' are elliptic curves over $\mathbb{Q}$ and $\phi\colon E \to E'$ is an isogeny over $\mathbb{Q}$. Then

$$\exists c > 0 \quad \forall P \in E(\mathbb{Q}) \quad |h(\phi(P)) - \deg(\phi)h(P)| \le c.$$

Proof. Recall Lemma 5.4,

$$\begin{array}{ccc} E & \xrightarrow{\phi} & E' \\ {\scriptstyle x}\downarrow & & \downarrow{\scriptstyle x} \\ \mathbb{P}^1 & \xrightarrow{\xi} & \mathbb{P}^1 \end{array}$$

where $\xi(X) = r(X)/s(X)$ for $r, s \in \mathbb{Q}[X]$ coprime and $\deg(\phi) = \max\{\deg(r),\deg(s)\} = d$, say.

By Corollary 12.2, there exist $c_1, c_2 > 0$ such that $c_1 H(P)^d \le H(\phi(P)) \le c_2 H(P)^d$. Taking logarithms, there exists a constant $c > 0$ such that $|h(\phi(P)) - dh(P)| \le c$ for all $P \in E(\mathbb{Q})$. □

Example. Consider $\phi = [2]\colon E \to E$. This gives that, for all $P \in E(\mathbb{Q})$,

$$|h(2P) - 4h(P)| \leq c.$$

Definition. The *canonical height* is

$$\hat{h}(P) = \lim_{n\to\infty} 4^{-n} h(2^n P).$$

We must check converges. If we let $m \geq n$ then

$$\begin{aligned}\left|\frac{1}{4^m}h(2^m P) - \frac{1}{4^n}h(2^n P)\right| &\leq \sum_{r=n}^{m-1}\left|\sum_{1} 4^{r+1}h(2^{r+1}P) - \frac{1}{4^r}h(2^r P)\right| \\ &\leq \sum_{r=n}^{m-1}\frac{1}{4^{r+1}}\left|h(2(2^r P)) - 4h(2^r P)\right| \\ &\leq c\sum_{r=n}^{\infty}\frac{1}{4^{r+1}} = c\frac{1}{4^{n+1}}\frac{1}{1-1/4} = \frac{c}{3\cdot 4^n} \to 0\end{aligned}$$

as $n \to \infty$. So this is a Cauchy sequence and $\hat{h}(P)$ is well-defined.

Lemma 12.4. (i) $|\hat{h}(P) - h(P)|$ is bounded independently of $P \in E(\mathbb{Q})$.
(ii) For any $B \geq 0$, $\{P \in E(\mathbb{Q}) : \hat{h}(P) \leq B\}$ is finite.

Proof. (i) Putting $n = 0$ in the above calculation gives

$$\left|\frac{1}{4^m}h(2^m P) - h(P)\right| \leq \frac{c}{3}.$$

Now take $m \to \infty$.

(ii) $\hat{h}(P)$ is bounded so $h(P)$ is bounded and hence $H(P)$ is bounded. Thus there are only finitely many choices for x and hence only finitely many choices for P.

□

Lemma 12.5. Suppose $\phi\colon E \to E'$ is an isogeny over $\mathbb{Q}$. Then

$$\forall P \in E(\mathbb{Q}) \quad \hat{h}(\phi(P)) = \deg(\phi)\hat{h}(P).$$

Proof. By Lemma 12.3, there exists a constant $c > 0$ such that

$$|h(2\phi(P)) - \deg(\phi)h(2^n P)| < c.$$

Now replace P by $2^n P$, divide by 4^n and let $n \to \infty$. □

Example. (i) $\phi = [n]\colon E \to E$ gives $\hat{h}(nP) = n^2\hat{h}(P)$ for all $P \in E(\mathbb{Q})$.
(ii) $h(P)$ depends on the Weierstrass equation, $\hat{h}(P)$ does not.
(iii) Here is another proof that $E(\mathbb{Q})_{tors}$ is finite: Let $P \in E(\mathbb{Q})_{tors}$, so $nP = \mathcal{O}_E$ for some $n \geq 1$. Thus $n^2\hat{P} = \hat{h}(nP) = \hat{h}(\mathcal{O}_E) = 0$ so $\hat{h}(P) = 0$. Now use Lemma 12.4 (ii).

Lemma 12.6. Let E be an elliptic curve over $\mathbb{Q}$. Then there exists a constant $c > 0$ such that

$$H(P \oplus Q)H(P \ominus Q) \leq cH(P)^2H(Q)^2.$$

for all $P, Q \in E(\mathbb{Q})$.

Proof. Assume $P, Q, P \oplus Q, P \ominus Q \neq \mathcal{O}_E$. Let $P = (x_1, y_1)$, $Q = (x_2, y_2)$, $P \oplus Q = (x_3, y_3)$ and $P \ominus Q = (x_4, y_4)$. Recall the explicit formulae for $x_3 + x_4$ and $x_3 x_4$ in terms of x_1 and x_2. Put $x_i = r_i/s_i$ with $r_i, s_i \in \mathbb{Z}$ coprime.

The argument is then a repeat of Lemma 5.6. □

Theorem 12.7. The map $\hat{h} \colon E(\mathbb{Q}) \to \mathbb{R}_{\geq 0}$ is a quadratic form.

Proof. Lemma 12.6 and the identity $\hat{h}(2P) = 4\hat{P}$ imply that

$$h(P \oplus Q) + h(P \ominus Q) \leq 2h(P) + 2h(Q) + C$$

for some constant C and all $P, Q \in E(\mathbb{Q})$. Now replace P and Q by $2^n P$ and $2^n Q$, respectively. Dividing by 4^n and taking the limit as $n \to \infty$, we have that

$$\hat{h}(P \oplus Q) + \hat{h}(P \ominus Q) \leq 2\hat{h}(P) + 2\hat{h}(Q).$$

Replacing P and Q by $P \oplus Q$ and $P \ominus Q$, respectively, gives the reverse inequality, so $\hat{h}$ satisfies the parallelogram law, so $\hat{h}$ is a quadratic form. □

For $x \in \mathbb{Q}^*$, define $|x|_p = p^{-\operatorname{ord}_p(x)}$, $|x|_\infty = |x|$. Then we have the product formula

$$\prod_v |x|_v = 1.$$

Definition. If $P = (x_0 : \cdots : x_n) \in \mathbb{P}^n(\mathbb{Q})$ define

$$H(P) = \prod_v \max\{|x_0|_v, \ldots, |x_n|_v\}.$$

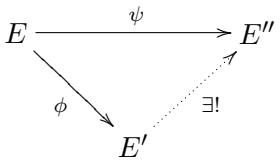
This is well-defined by the product formula. Moreover, it can be extended to a definition over number fields.

Chapter 13

Dual Isogenies

For now, assume that K is a perfect field, E an elliptic curve over K and $G = \mathrm{Gal}(\bar{K}, K)$.

Proposition 13.1. Suppose $\Phi \subset E(\bar{K})$ is a finite G-stable group. Then there exists an elliptic curve E'/K and a separable isogeny $\phi\colon E \to E'$, defined over K, such that every isogeny $\psi\colon E \to E''$ with $\Phi \subset \ker(\psi)$ factors uniquely via ϕ:



Sketch of proof. The basic idea is as follows. $E' = E/\Phi$ has function field $K(E)^{\Phi}$ where $P \in \Phi$ acts on $K(E)$ as τ_P^*, where $\tau_P\colon E \to E$ is the translation by P. □

Proposition 13.2. Let $\phi\colon E \to E'$ be an isogeny of degree n. Then there exists a unique isogeny $\hat{\phi}\colon E' \to E$, called the *dual isogeny*, such that $\hat{\phi}\phi = [n]$.

Proof. (*Existence.*) We only consider the case that ϕ is separable. Then $|E[\phi]| = \deg(\phi) = n$ and hence $E[\phi] \subset E[n]$. Now apply Proposition 13.1 to $\psi = [n]$.

The case that ϕ is inseparable is omitted, however, the result is not used in the course.

(*Uniqueness.*) Suppose $\psi_1, \psi_2\colon E' \to E$ are such that $\psi_1\phi = [n] = \psi_2\phi$. Then $(\psi_1 - \psi_2)\phi = 0$. Now morphisms of algebraic curves are surjective or constant. Hence $\psi_1 - \psi_2 = 0$ and $\psi_1 = \psi_2$. □

Remark.
(i) If $\deg[n] = n^2$ then $\deg(\phi) = \deg(\hat{\phi})$ and $[\hat{n}] = [n]$.
(ii) $\phi\hat{\phi}\phi = \phi[\deg(\phi)] = [\deg(\phi)]\phi$ so $(\phi\hat{\phi} - [\deg(\phi)])\phi = 0$ and so $\phi\hat{\phi} = [\deg(\phi)]$, hence $\hat{\hat{\phi}} = \phi$.
(iii) E and E' are isogeneous over K if there exists an isogeny $\phi\colon E \to E'$ defined over K. This is an equivalence relation.
(iv) If $\phi, \psi \in \mathrm{Hom}(E, E')$ then we can show that $\widehat{\phi + \psi} = \hat{\phi} + \hat{\psi}$.

Chapter 14

Galois Cohomology

Suppose that G is a group and A a G-module.

Definition. Set $H^0(G,A) = A^G = \{a \in A : \forall \sigma \in G \quad \sigma(a) = a\}$. We also define the sequence $B^1(G,A) \subset Z^1(G,A) \subset C^1(G,A)$ by

$$\begin{aligned} C^1(G,A) &= \{\text{maps } G \to A\}, \\ Z^1(G,A) &= \{(a_\sigma)_{\sigma\in G} : \forall \sigma,\tau \in G \quad a_{\sigma\tau} = \sigma(a_\tau) + a_\sigma\}, \\ B^1(G,A) &= \{(\sigma(b) - b)_{\sigma\in G} : b \in A\}. \end{aligned}$$

We call $C^1(G,A)$ *chains* and $Z^1(G,A)$ *cocycles*.

Definition. Set $H^1(G,A) = Z^1(G,A)/B^1(G,A)$.

Remark. If G acts trivially on A then $H^1(G,A) = \mathrm{Hom}(G,A)$.

Theorem 14.1. Let $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ be a short exact sequence of G-modules. Then there exists a long exact sequence of abelian groups

$$0 \to A^G \to B^G \to C^G \xrightarrow{\delta} H^1(G,A) \to H^1(G,B) \to H^1(G,C).$$

Proof. Omitted. But we give the construction of δ. Let $c \in C^G$. Then there exists a $b \in B$ such that $g(b) = c$. For all $\sigma \in G$, $g(\sigma(b) - b) = \sigma(g(b)) - g(b) = \sigma(c) - c = 0$ so $\sigma(b) - b = f(a_\sigma)$ for some $a_\sigma \in A$. Now check that $(a_\sigma)_{\sigma\in G} \in Z^1(G,A)$ and define $\delta(c)$ to be the class of (a_σ) in $H^1(G,A)$. □

Theorem 14.2. Let A be a G-module and $H \triangleleft G$ be a normal subgroup. Then there exists an inflation-restriction exact sequence

$$0 \to H^1(G/A, A^H) \xrightarrow{\inf} H^1(G,A) \xrightarrow{\mathrm{res}} H^1(H,A).$$

Proof. Omitted. □

Theorem 14.3 (Hilbert's Theorem 90)**.** If L/K is a finite Galois extension then $H^1(\mathrm{Gal}(L/K), L^*) = 0$.

Proof. Take $(a_\sigma)_{\sigma\in G} \in Z^1(G, L^*)$ where $G = \mathrm{Gal}(L/K)$. Distinct automorphisms are linearly independent so there exists $y \in L^*$ such that

$$x = \sum_{\tau\in G} a_\tau^{-1}\tau(y) \neq 0.$$

If $\sigma \in G$ then

$$\sigma(x) = \sum_{\tau\in G} \sigma(a_\tau)^{-1}\sigma\tau(y) = a_\sigma \sum_{\tau\in G} a_{\sigma\tau}^{-1}\sigma\tau(y) = a_\sigma x$$

so $a_\sigma = \sigma(x)/x$ and hence $(a_\sigma) \in B^1(G, L^*)$. Therefore, $Z^1(G, L^*) = B^1(G, L^*)$ and finally $H^1(G, L^*) = 0$. □

Now suppose that K is perfect. $\mathrm{Gal}(\bar{K}, K)$ is a topological group with basis of open subgroups $\mathrm{Gal}(\bar{K}, L)$ for $[L : K] < \infty$. If $G = \mathrm{Gal}(\bar{K}, K)$ then we modify the definition of $H^1(G, A)$ by insisting that

(i) the stabiliser of $a \in A$ is an open subgroup of G,
(ii) all cochains are continuous, with the discrete topology on A.

Then

$$H^1(\mathrm{Gal}(\bar{K}, K), A) = \varinjlim_{L/K \text{ finite Galois}} H^1\Big(\mathrm{Gal}(L/K), A^{\mathrm{Gal}(\bar{K},L)}\Big),$$

the direct limit with respect to inflation maps.

14.1 Application to Kummer Theory

Suppose that $\mathrm{char}(K) \nmid n$. Then we have a short exact sequence of $\mathrm{Gal}(\bar{K}/K)$-modules

$$0 \to \mu_n \to \bar{K}^* \to \bar{K}^* \to 0$$

where the map $\bar{K}^* \to \bar{K}^*$ is $x \mapsto x^n$. We have the following long exact squence

$$K^* \to K^* \xrightarrow{\delta} H^1(\mathrm{Gal}(\bar{K}/K), \mu_n) \to H^1(\mathrm{Gal}(\bar{K}/K), \bar{K}^*) = 0,$$

where the first map is $x \mapsto x^n$ and the last identity is by Hilbert's Theorem 90. Therefore, $H^1(\mathrm{Gal}(\bar{K}/K), \mu_n) \cong K^*/(K^*)^n$.

If $\mu_n \subset K$ then we get

$$\mathrm{Hom}_{cts}(\mathrm{Gal}(\bar{K}/K), \mu_n) \cong K^*/(K^*)^n$$

and finite subgroups of the left-hand side are of the form $\mathrm{Hom}(\mathrm{Gal}(L/K), \mu_n)$ for L a finite extension of K of exponent dividing n. (See Proposition 10.2.)

Suppose $\phi\colon E \to E'$ is an isogeny of elliptic curves over K. We have the short exact sequence

$$0 \to E[\phi] \to E \xrightarrow{\phi} E' \to 0$$

and we can take the long exact sequence

$$0 \to E(K)[\phi] \to E(K) \xrightarrow{\phi} E'(K) \xrightarrow{\delta} H^1(\mathrm{Gal}(\bar{K}/K), E[\phi])$$
$$\to H^1(\mathrm{Gal}(\bar{K}/K), E) \xrightarrow{\phi} H^1(\mathrm{Gal}(\bar{K}/K), E')$$

so we obtain

$$0 \to E'(K)/\phi E(K) \to H^1(\mathrm{Gal}(\bar{K}/K), E[\phi]) \to H^1(\mathrm{Gal}(\bar{K}/K), E[\phi]) \to 0. \qquad (\dagger)$$

For a number field K let $M_K = \{\text{places of } K\}$, which can be divided into finite places, i.e., prime ideals of $\mathcal{O}_K$, and infinite places, i.e., embeddings $K \hookrightarrow \mathbb{R}$ or pairs of embeddings $K \hookrightarrow \mathbb{C}$.

For $v \in M_K$ we have the completion $K_v \supset K$. Fix an embedding $\bar{K} \subset \bar{K}_v$. Then $\mathrm{Gal}(\bar{K}_v/K) \subset \mathrm{Gal}(\bar{K}/K)$ and $E(\bar{K}) \subset E(\bar{K}_v)$. So from (†) we obtain the diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & E'(K)/\phi E(K) & \xrightarrow{\delta_\phi} & H^1(\mathrm{Gal}(\bar{K}/K), E[\phi]) & \longrightarrow & H^1(\mathrm{Gal}(\bar{K}/K), E[\phi]) & \longrightarrow & 0 \\
 & & & & \downarrow{\scriptstyle \mathrm{res}_v} & \searrow & & & \\
0 & \longrightarrow & E'(K_v)/\phi E(K_v) & \xrightarrow{\delta_{\phi,r}} & H^1(\mathrm{Gal}(\bar{K}_v/K_v), E[\phi]) & \longrightarrow & H^1(\mathrm{Gal}(\bar{K}_v/K_v), E[\phi]) & \longrightarrow & 0
\end{array}$$

Definition. The *ϕ-Selmer group* is

$$\begin{aligned} S^{(\phi)} &= \ker\Big(H^1(\mathrm{Gal}(\bar{K}/K), E[\phi]) \to \prod_{v \in M_K} H^1(\mathrm{Gal}(\bar{K}_v/K_v), E)\Big) \\ &= \{x \in H^1(\mathrm{Gal}(\bar{K}/K), E[\phi]) : \forall v \in M_K \quad \mathrm{res}_v(x) \in \mathrm{Im}(\delta_{\phi,v})\}. \end{aligned}$$

The *Tate–Shafarevich group* of E is

$$Ш(E/K) = \ker\Big(H^1(\mathrm{Gal}(\bar{K}/K), E) \to \prod_{v \in M_K} H^1(\mathrm{Gal}(\bar{K}_v/K), E)\Big).$$

Thus the previous diagram gives the short exact sequence

$$0 \to E'(K)/\phi E(K) \to S^{(\phi)}(E/K) \to Ш(E/K)[\phi] \to 0.$$

where $Ш(E/K)[\phi] = \ker\big(Ш(E/K) \xrightarrow{\phi} Ш(E'/K)\big)$.

The proof of Weak Mordell–Weil may be rearranged to give the following theorem.

Theorem 14.4. $S^{(\phi)}(E/K)$ is finite.

Corollary 14.5. (i) $E'(K)/\phi E(K)$ is finite.
(ii) $Ш(E/K)[\phi]$ is finite.

Conjecture. $Ш(E/K)$ is finite.

Definition. Let $S \subset M_K$ be a finite set of places containing all infinite places. Then set

$$H^1(K, E[\phi]; S) = \ker\Big(H^1(\mathrm{Gal}(\bar{K}/K), E[\phi]) \to \prod_{v \notin S} H^1(\mathrm{Gal}(\bar{K}_v/K_v^{nr}), E[\phi])\Big)$$

and note that $\mathrm{Gal}(\bar{K}_v/K_v^{nr}) \subset \mathrm{Gal}(\bar{K}_v/K_v) \subset \mathrm{Gal}(\bar{K}/K)$.

Lemma 14.6. Take $S = \{\text{bad primes for } E\} \cup \{p : p \mid \deg(\phi)\} \cup \{\text{infinite places}\}$. Then $S^{(\phi)}(E/K) \subset H^1(K, E[\phi]; S)$.

Proof. Let $n = \deg(\phi)$. Take $v \notin S$, then $E(K_v^{nr}) \xrightarrow{\times n} E(K_v^{nr})$ is surjective by Proposition 8.11. Thus, the map $E(K_v^{nr}) \xrightarrow{\phi} E'(K_v^{nr})$ is also surjective since $\phi\hat{\phi} = [n]$. We have the following diagram:

$$\begin{array}{ccccc} E(K_v) & \xrightarrow{\phi} & E'(K_v)\delta_{\phi,r} & \longrightarrow & H^1\big(\mathrm{Gal}(\bar{K}_v/K_v), E[\phi]\big) \\ \big| & & \big| & & \big\downarrow \mathrm{res}_v \\ E(K_v^{nr} & \xrightarrow{\phi} & E'(K_v^{nr}) & \longrightarrow & H^1\big(\mathrm{Gal}(\overline{K_v^{nr}}/K_v^{nr}\big), E[\phi]\big) \end{array}$$

This shows that $x \in S^{(\phi)}(E/K)$ and so $\mathrm{res}_v(x) \in \mathrm{Im}(\delta_{\phi,v})$. Hence the image of x in $H^1\big(\mathrm{Gal}(\bar{K}_v/K_v^{nr}), E[\phi]\big)$ is trivial. □

Recall that K is a number field, S a finite set of places including all infinite places and A a finite topological $\mathrm{Gal}(\bar{K}/K)$-module.

Lemma 14.7. *$H^1(K, A; S)$ is finite.*

Proof. If L/K is finite Galois, we have an exact sequence given by

$$0 \to H^1\big(\mathrm{Gal}(L/K), A^{\mathrm{Gal}(\bar{K}/L)}\big) \underset{\inf}{\longrightarrow} H^1(K, A) \xrightarrow{\mathrm{res}} H^1(L, A)$$

and note that $H^1(K, A; S) \subset H^1(K, A)$. So we are free to extend K.

Without loss of generality, $\mathrm{Gal}(\bar{K}/K)$ acts trivially on A. Noting that $H^1(K, A_1 \times A_2) \cong H^1(K, A_1) \times H^1(K, A_2)$, we may also assume that A is cyclic, say of order n. Moreover, without loss of generality, $\mu_n \subset K$ so that $A \cong \mu_n$ as a Galois module. It suffices to show that $H^1(K, \mu_n; S)$ is finite.

By Hilbert's Theorem 90, $H^1(K, \mu_n) \cong K^*/(K^*)^n$ and now

$$H^1(K, \mu_n; S) = \ker\Big(K^*/(K^*)^n \to \prod_{v \notin S} (K_v^{nr})^* \,/\, \big((K_v^{nr})^*\big)^n\Big) \subset K(S, n)$$

which is finite by Proposition 9.6. □

Lemmas 14.6 and 14.7 imply that $S^{(\phi)}(E/K)$ is finite.

Proof of Lemma 11.3. Suppose that L/K is finite Galois. Then

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^1(\mathrm{Gal}(L/K), E(L)[n]) & \underset{\inf}{\longrightarrow} & H^1(K, E[n]) & \xrightarrow{\mathrm{res}} & H^1(L, E[n]) \\ & & & & \big\uparrow & & \big\uparrow \\ & & & & E(K)/nE(K) & & E(L)/nE(L) \end{array}$$

Thus $|E(K)/nE(K)| < \infty$ whenever $|E(L)/nE(L)| < \infty$. □

Chapter 15

Weil Pairing

We recall Corollary 4.3, stating that $D \in \mathrm{Div}(E)$ is principal if and only if $\deg(D) = 0$ and $\mathrm{sum}(D) = \mathcal{O}_E$.

Suppose that $\phi\colon E \to E'$ is an isogeny of degree n with dual $\hat{\phi}\colon E' \to E$ so that $\hat{\phi}\phi = [n]_E$ and $\phi\hat{\phi} = [n]_{E'}$. Let us assume that $\mathrm{char}(K) \nmid n$. We define the *Weil pairing* $e_\phi\colon E[\phi] \times E'[\hat{\phi}] \to \mu_n$ as follows.

Let $T \in E'[\hat{\phi}]$. Then $nT = \mathcal{O}_{E'}$ and there exists $f \in \bar{K}(E')^*$ such that

$$\mathrm{div}(f) = n(T) - n(\mathcal{O}_{E'}) \tag{1}$$

and

$$\mathrm{div}(\phi^*(f)) = \phi^*(\mathrm{div}(f)) = n(\phi^*(T) - \phi^*(\mathcal{O}_{E'})).$$

Pick $T_0 \in E$ such that $\phi(T_0) = T$. So

$$\phi^*(T) - \phi^*(\mathcal{O}_{E'}) = \sum_{S' \in E[\phi]} (S' + T_0) - \sum_{S' \in E[\phi]} (S').$$

Observe that the degree of the right-hand side is 0 and the sum is $[n]T_0 = \hat{\phi}\phi(T_0) = \hat{\phi}(T) = \mathcal{O}_{E'}$. Thus, there exists $g \in \bar{K}[E]^*$ such that $\mathrm{div}(g) = \phi^*(T) - \phi^*(\mathcal{O}_{E'})$. Then $\mathrm{div}(\phi^*(f)) = n\,\mathrm{div}(g) = \mathrm{div}(g^n)$ and so $\phi^*(f) = cg^n$ for some $c \in \bar{K}^*$. Rescaling f, we may assume that $c = 1$. So

$$\phi^*(f) = g^n. \tag{2}$$

Let $S \in E[\phi]$. Then $\tau_S^*(\mathrm{div}(g)) = \mathrm{div}(g)$, so $\mathrm{div}(\tau_S^*(g)) = \mathrm{div}(g)$ and hence $\tau_S^*(g) = \zeta g$ for some $\zeta \in \bar{K}^*$, that is,

$$\zeta^n = \frac{g(X+S)^n}{g(X)^n} = \frac{f(\phi(X+S))}{f(\phi(X))} = 1$$

as $\phi(S) = \mathcal{O}_{E'}$. So $\zeta \in \mu_n$. Define $e_\phi(S,T) = g(X+S)/g(X) = \zeta$.

Proposition 15.1. e_ϕ is bilinear and non-degenerate.

Proof. We begin by showing linearity in the first argument.

$$e_\phi(S_1+S_2,T) = \frac{g(X+S_1+S_2)}{g(X)} = \frac{g(X+S_1+S_2)}{g(X+S_2)}\frac{g(X+S_2)}{g(X)} = e_\phi(S_1,T)e_\phi(S_2,T)$$

For the second argument, let $T_1, T_2 \in E'[\hat{\phi}]$ and observe that

$$\begin{aligned} \operatorname{div}(f_1) &= n(T_1) - n(\mathcal{O}_{E'}), \qquad \phi^*(f_1) = g_1^n, \\ \operatorname{div}(f_2) &= n(T_2) - n(\mathcal{O}_{E'}), \qquad \phi^*(f_2) = g_2^n \end{aligned}$$

and there exists $h \in \bar{K}(E')$ such that $\operatorname{div}(h) = (T_1) + (T_2) - (T_1 \oplus T_2) - (\mathcal{O}_{E'})$. Now set $f = f_1 f_2 / h^n$ and $g = g_1 g_2 / \phi^*(h)$ and check that

$$\begin{aligned} \operatorname{div}(f) &= n(T_1 + T_2) - n(\mathcal{O}_{E'}), \\ \phi^*(f) &= \frac{\phi^*(f_1)\phi^*(f_2)}{\phi^*(h)^n} = \frac{g_1^n g_2^n}{\phi^*(h)^n} = g^n. \end{aligned}$$

Then, for $S \in E[\phi]$,

$$e_\phi(S, T_1 + T_2) = \frac{g(X+S)}{g(X)} = \frac{g_1(X+S)}{g_1(X)} \frac{g_2(X+S)}{g_2(X)} \frac{h(\phi(X))}{h(\phi(X+S))} = e_\phi(S, T_1) e_\phi(S, T_2)$$

as $\phi(S) = \mathcal{O}_{E'}$.

We now show that ϕ is non-degenerate. Fix $T \in E'[\hat{\phi}]$. Suppose $e_\phi(S, T) = 1$ for all $S \in E[\phi]$. Then $\tau_S^*(g) = g$ for all $S \in E[\phi]$. We have that $\bar{K}(E)/\phi^*\bar{K}(E')$ is a Galois extension with Galois group $E[\phi]$ and $S \in E[\phi]$ acts as τ_S^*. Therefore, $g = \phi^*(h)$ for some $h \in \bar{K}(E')$ so $\phi^*(f) = g^n = \phi^*(h^n)$ and hence $f = h^n$. But $\operatorname{div}(f) = n(T) - n(\mathcal{O}_{E'})$ so $\operatorname{div}(h) = (T) - (\mathcal{O}_{E'})$, hence $T = \mathcal{O}_{E'}$.

Now $|E[\phi]| = |E'[\hat{\phi}]| = n$, so e_ϕ is non-degenerate. □

Lemma 15.2. If E, E' and ϕ are defined over K then e_ϕ is *Galois equivariant*, that is, $e_\phi(\sigma(S), \sigma(T)) = \sigma(e_\phi(S, T))$ for all $\sigma \in \operatorname{Gal}(\bar{K}/K)$.

Proof. From the definition of e_ϕ we have that

$$\operatorname{div}(f) = n(T) - n(\mathcal{O}_{E'}), \qquad \phi^*(f) = g^n$$

so that

$$\operatorname{div}(\sigma f) = n(\sigma(T)) - n(\mathcal{O}_{E'}), \qquad \phi^*(\sigma f) = \sigma(g)^n.$$

This gives that

$$\begin{aligned} e_\phi(\sigma(S), \sigma(T)) &= \frac{(\sigma g)(\sigma(S) + X)}{(\sigma g)(X)} \\ &= \frac{(\sigma g)(\sigma(S) + \sigma(X))}{(\sigma g)(\sigma(X))} \\ &= \sigma\left(\frac{g(S+X)}{g(X)}\right) \\ &= \sigma(e_\phi(S, T)). \end{aligned}$$

□

Taking $\phi = [n] \colon E \to E$, we have $e_n \colon E[n] \times E[n] \to \mu_n$.

Fact. e_n is alternating, that is, $e_n(T, T) = 1$ for all T.

Corollary 15.3. Assume that $\operatorname{char}(K) \nmid n$. If $E(K)[n] = E(\bar{K})[n]$ then $\mu_n \subset K$.

Proof. Pick $S \in E(\bar{K})[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$ of order n. e_n is non-degenerate, so there exists $T \in E[n]$ such that $e_n(S,T) = \zeta_n$ is a primitive nth root of unity. Then

$$\sigma(\zeta_n) = \sigma(e_n(S,T)) = e_n(\sigma(S), \sigma(T)) = e_n(S,T) = \zeta_n$$

for all $\sigma \in \mathrm{Gal}(\bar{K}/K)$ so $\zeta_n \in K$ and hence $\mu_n \subset K$. □

Example. There does not exist an elliptic curve $E/\mathbb{Q}$ such that $E(\mathbb{Q})_{tors} \cong (\mathbb{Z}/3\mathbb{Z})^2$.

Chapter 16

Decent by Cyclic Isogeny

Suppose that K is a number field and $\phi\colon E \to E'$ an isogeny over K. Recall that $S^{(\phi)}(E/K) \subset H^1(K, E[\phi])$. Suppose that $E'[\hat{\phi}] \cong \mathbb{Z}/n\mathbb{Z}$, generated by $T \in E'(K)$. Then $E[\phi] \cong \mu_n$ via $S \mapsto e_\phi(S, T)$, respecting the action of Galois. We have the short exact sequence

$$0 \to \mu_n \to E \xrightarrow{\phi} E' \to 0$$

giving the long exact sequence

$$\begin{array}{ccccccc} E(K) & \xrightarrow{\phi} & E'(K) & \xrightarrow{\delta} & H^1(K, \mu_n) & \longrightarrow & H^1(K, E) \\ & & & \searrow^{\alpha} & \downarrow \cong & & \\ & & & & K^*/(K^*)^n & & \end{array}$$

where the isomorphism is given by Hilbert's Theorem 90.

Proposition 16.1. Let $f \in K(E')$ and $g \in K(E)$ with

$$\operatorname{div}(f) = n(T) - n(\mathcal{O}_{E'}), \qquad \phi^*(f) = g^n.$$

Then $\alpha(P) \equiv f(P) \pmod{(K^*)^n}$ for all $P \in E'(K) - \{\mathcal{O}_{E'}, T\}$.

Proof. Pick $Q \in E(\bar{K})$ such that $\phi(Q) = P$. Then $\delta(P)$ is represented by the cocycle $(\sigma \mapsto \sigma(Q) - Q)$ where $\sigma(Q) - Q \in E[\phi] \cong \mu_n$. We have

$$\begin{aligned} e_\phi(\sigma(Q) - Q, T) &= \frac{g(X + \sigma(Q) - Q)}{g(X)} \\ &= \frac{g(\sigma(Q))}{g(Q)} = \frac{(\sigma g)(Q)}{g(Q)} = \frac{\sigma\big(\sqrt[n]{f(P)}\big)}{\sqrt[n]{f(P)}} \end{aligned}$$

where the first equality holds for all $X \in E$ except zeros and poles of g, since $\phi^*(f) = g^n$ and $\phi(Q) = P$.

Recalling $K^*/(K^*)^n \cong H^1(K, \mu_n)$ via $x \mapsto \big(\sigma \mapsto \sigma(\sqrt[n]{x})/\sqrt[n]{x}\big)$, it follows that $\alpha(P) \equiv f(P) \pmod{(K^*)^n}$. □

From now, let us take $n = 2$. We consider the pair of elliptic curves

$$E\colon y^2 = x^3 + ax^2 + bx, \qquad E'\colon y^2 = x^3 + a'x^2 + b'x$$

with $a' = -2a$ and $b' = a^2 - 4b$. (See Example Sheet 2.) We consider the following isogeny:

$$\phi\colon E \to E', (x,y) \mapsto \left(\frac{y^2}{x^2}, \frac{y(x^2-b)}{x^2}\right)$$
$$\hat{\phi}\colon E' \to E, (x,y) \mapsto \left(\frac{y^2}{4x^2}, \frac{y(x^2-b')}{8x^2}\right)$$

with $E[\phi] = \{\mathcal{O}_E, T\}$, $T = (0,0)$ and $E'[\hat{\phi}] = \{\mathcal{O}_{E'}, T'\}$, $T' = (0,0)$. We can check that $\hat{\phi}\phi = [2]_E$ and $\phi\hat{\phi} = [2]_{E'}$.

Proposition 16.2. The map $\alpha_{E'}\colon E'(K) \to K^*/(K^*)^2$ given by

$$(x,y) \mapsto \begin{cases} x & x \neq 0 \\ b' & x = 0 \end{cases}$$

is a group homomorphism with kernel $\phi(E(K))$.

Proof. Either apply Proposition 16.1 with $f = x \in K(E')$ and $g = y/x \in K(E)$ or perform a direct calculation, see Example Sheet 4. □

Lemma 16.3. With the above notation we have that

$$2^{\operatorname{rank} E(K)} = \frac{1}{4}|\operatorname{Im}\alpha_E||\operatorname{Im}\alpha_{E'}|.$$

Proof. Since $\phi\hat{\phi} = [2]_{E'}$ and $\hat{\phi}\phi = [2]_E$ we have the exact sequence

$$0 \to E(K)[\phi] \to E(K)[2] \xrightarrow{\phi} E'(K)[\hat{\phi}]$$
$$\to E'(K)/\phi E(K) \xrightarrow{\phi} E(K)/2E(K) \to E(K)/\hat{\phi}E'(K) \to 0.$$

As $E'(K)/\phi E(K) \cong \operatorname{Im}\alpha_{E'}$ and $E(K)/\hat{\phi}E'(K) \cong \operatorname{Im}\alpha_E$, we deduce that

$$\frac{|E(K)/2E(K)|}{|E(K)[2]|} = \frac{1}{4}|\operatorname{Im}\alpha_E||\operatorname{Im}\alpha_{E'}|.$$

By Mordell–Weil, we can write $E(K) \cong \Delta \times \mathbb{Z}^r$ with Δ finite. Thus

$$E(K)/2E(K) \cong \Delta/2\Delta \times (\mathbb{Z}/2\mathbb{Z})^r$$

and $E(K)[2] \cong \Delta[2]$. As Δ is finite, $|\Delta/2\Delta| = |\Delta[2]|$. Hence

$$\frac{|E(K)/2E(K)|}{|E(K)[2]|} = 2^r.$$ □

Lemma 16.4. Suppose K is a number field and $a, b \in \mathcal{O}_K$. Then $\operatorname{Im}\alpha_E \subset K(S,2)$, where S is the set of primes dividing b.

Proof. We must show that if $x, y \in K$ with $y^2 = x(x^2 + ax + b)$ and $\operatorname{ord}_p(b) = 0$ then $\operatorname{ord}_p(x) \equiv 0 \pmod 2$. We consider two cases.

If $\operatorname{ord}_p(x) < 0$ then, by Lemma 8.1, $\operatorname{ord}_p(x) = -2r$ and $\operatorname{ord}_p(y) = -3r$. If $\operatorname{ord}_p(x) > 0$ then $\operatorname{ord}_p(x^2 + ax + b) = 0$ so $\operatorname{ord}_p(x) = \operatorname{ord}_p(y^2) = 2\operatorname{ord}_p(y)$. □

Lemma 16.5. If $b_1b_2 = b$ then $b_1(K^*)^2 \in \operatorname{Im}\alpha_E$ if and only if the equation

$$w^2 = b_1u^4 + au^2v^2 + b_2v^4 \qquad (*)$$

is soluble for $u, v, w \in K$ not all zero.

Proof. If b_1 or b_2 is in $(K^*)^2$ then both conditions are satisfied. So suppose that $b_1, b_2 \notin (K^*)^2$, then $b_1(K^*)^2 \in \operatorname{Im}\alpha_E$ if and only if

$$\exists (x,y) \in E(K) \quad \exists t \in K^* \quad x = b_1t^2.$$

Then

$$y^2 = b_1t^2\big((b_1t^2)^2 + a(b_1t^2) + b\big)$$

and hence

$$\Big(\frac{y}{b_1t}\Big)^2 = b_1t^4 + at^2 + b_2$$

i.e., equation $(*)$ has the solution $(u, v, w) = (t, 1, y/b_1t)$.

Conversely, if equation $(*)$ has solution (u, v, w) with $uv \neq 0$ then

$$\Big(b_1\Big(\frac{u}{v}\Big)^2, b_1\frac{uw}{v^3}\Big) \in E(K)$$

so $b_1(K^*)^2 \in \operatorname{Im}\alpha_E$. □

Corollary 16.6.

$$S^{(\hat{\phi})}(E'/K) = \big\{b_1(K^*)^2 \in K^*/(K^*)^2 : (*) \text{ has a solution over } K_v \text{ for all places } v\big\}.$$

Example. Let $K = \mathbb{Q}$ and consider $E\colon y^2 = x^3 - x$, $b = -1$. Then

$$\operatorname{Im}\alpha_E \subset \langle -1\rangle \subset \mathbb{Q}^*/(\mathbb{Q}^*)^2.$$

But $-1 \in \operatorname{Im}\alpha_E$ so $\operatorname{Im}\alpha_E = \langle -1\rangle$. We have

$$E'\colon y^2 = x^3 + 4x, \qquad b' = 4$$

so that $\operatorname{Im}\alpha_{E'} \subset \langle -1, 2\rangle \subset \mathbb{Q}^*/(\mathbb{Q}^*)^2$ and we consider three cases: If $b_1 = -1$ then we see that $w^2 = -u^4 - 4v^4$ has no solutions over $\mathbb{R}$. If $b_1 = 2$ then the equation is $w^2 = 2u^4 + v^4$ and this has solution $(u, v, w) = (1, 1, 2)$. Finally, $b_1 = -2$ gives $w^2 = -2u^4 - 2v^4$, which has no solutions over $\mathbb{R}$. Thus $\operatorname{Im}\alpha_{E'} = \langle 2\rangle \subset \mathbb{Q}^*/(\mathbb{Q}^*)^2$ and so

$$2^{\operatorname{rank} E(\mathbb{Q})} = \frac{2\cdot 2}{4} = 1$$

so $\operatorname{rank} E(\mathbb{Q}) = 0$. We deduce that 1 is not a congruent number.

Example. Consider $E\colon y^2 = x^3 + px$ with $p \equiv 5 \pmod 8$ a prime. We note that $b_1 = -1$ leads to $w^2 = -u^4 - pv^4$, which has no solution over $\mathbb{R}$. This gives $\operatorname{Im}\alpha_E = \langle p\rangle \subset \mathbb{Q}^*/(\mathbb{Q}^*)^2$.

We have $E'\colon y^2 = x^3 - 4px$ which has

$$\operatorname{Im}\alpha_{E'} \subset \langle -1, 2, p\rangle \subset \mathbb{Q}^*/(\mathbb{Q}^*)^2.$$

Now $\alpha_{E'}(0,0) = (-p)(\mathbb{Q}^*)^2$ and we consider three cases:

$$b_1 = 2 \quad \Longrightarrow \quad w^2 = 2u^4 - 2pv^4, \tag{1}$$
$$b_1 = -2 \quad \Longrightarrow \quad w^2 = -2u^4 + 2pv^4, \tag{2}$$
$$b_1 = p \quad \Longrightarrow \quad w^2 = pu^4 - 4pv^4. \tag{3}$$

Suppose that $u, v, w \in \mathbb{Q}$ satisfy (1). We may assume that $u, v \in \mathbb{Z}$ are coprime. If $p \mid u$ then $p \mid w$ so $p \mid v$, contradiction. Thus $w^2 \equiv 2u^4 \not\equiv 0 \pmod{p}$ and hence $2 \in (\mathbb{F}_p^*)^2$, contradicting $p \equiv 5 \pmod{8}$. So (1) has no solution. Likewise, equation (2) gives $-2 \in (\mathbb{F}_p^*)^2$, contradiction. So far, we have that $\operatorname{Im}\alpha_{E'} \subset \langle -1, p\rangle$. We conclude that $\operatorname{rank} E(\mathbb{Q})$ is 0 if (3) is insoluble and 1 if (3) is soluble.

p	u	v	w
5	1	1	1
13	1	1	3
29	1	1	5
37	5	3	15
53	1	1	7
61	5	9	109

Definition. Set $C\colon w^2 = b_1u^4 + au^2v^2 + b_2v^4$ and let $C(K)$ be the set of solutions with $u, v, w \in K$ not all zero.

Fact. If $a, b_1, b_2 \in \mathbb{Z}$ and $p \nmid 2b(a^2 - 4b)$ then $C(\mathbb{Q}_p) \neq \emptyset$.

Example (Lind)**.** Let $E\colon y^2 = x^3 + 17x$. Then $\operatorname{Im}\alpha_E = \langle 17\rangle \subset \mathbb{Q}^*/(\mathbb{Q}^*)^2$ and as $E'\colon y^2 = x^3 - 4 \cdot 17x$ so that $\operatorname{Im}\alpha_{E'} \subset \langle -1, 2, 17\rangle \subset \mathbb{Q}^*/(\mathbb{Q}^*)^2$.

Considering $b_1 = 2$, we have $w^2 = 2u^4 - 2 \cdot 17v^4$ and so, replacing w by $2w$, $C\colon 2w^2 = u^4 - 17v^4$. We find that $C(\mathbb{Q}_2) \neq \emptyset$ as $17 \in (\mathbb{Z}_2^*)^4$, $C(\mathbb{Q}_{17}) \neq \emptyset$ since $(2|17) = 1$ and $C(\mathbb{R}) \neq \emptyset$.

The above fact gives that $C(\mathbb{Q}_v) \neq \emptyset$ for all places v of $\mathbb{Q}$. Suppose that $(u, v, w) \in C(\mathbb{Q})$. Without loss of generality, $u, v, w \in \mathbb{Z}$ and $(u, v) = 1$. If $17 \mid w$ then $17 \mid u$ and so $17 \mid v$, contradiction. Suppose that $p \mid w$, then $(17|p) = 1$ so $(p|17) = (17|p) = 1$. So w is a square modulo 17. Then $2w^2 \equiv u^4 \pmod{17}$ and hence $2 \in (\mathbb{F}_{17}^*)^4 = \{\pm 1, \pm 4\}$, contradiction. So $C(\mathbb{Q}) = \emptyset$.